JESTT

Vol. 2, Issue. 1, 2025

SCOPUA

Journal of Engineering, Science and Technological Trends

ISSN(e): 2959-1937

Volume 2 (Issue 1) Published on 2025-02-28

https://doi.org/10.48112/jestt.v2i1

2025

Journal Homepage

https://journals.scopua.com/index.php/JESTT

Publisher

Scientific Collaborative Online Publishing Universal Academy

Publisher Homepage

https://scopua.com/

Model Town - Ferozepur Road, Near Atfaq Hospital, Lahore, Pakistan

Journal of Engineering, Science and Technological Trends

Aims and Scope

The Journal of Engineering, Science and Technological Trends (JESTT) is a double-blind-peer-reviewed, open-access wide-ranging journal for publishing novel primary research findings, reviews, and short communications throughout the broad gamut of engineering disciplines. The journal editorial board welcomes manuscripts in both fundamental and applied research areas and encourages submissions that contribute novel and innovative insights to engineering science and technology.

All submitted articles considered suitable for JESTT are subjected to rigorous double-blind peer review to ensure the highest levels of quality. The journal is highly interdisciplinary and welcomes scientifically robust research in traditional and emerging areas. Original papers which provide an essential contribution to the development of engineering sciences and report on significant developments in the field are encouraged. The review process is carried out as quickly as possible to minimize any delays in the online publication of articles.

JESTT aims to advance the understanding of engineering sciences by providing a platform for the publication of unique contributions in the field of engineering and technology across various topics, including, but not limited to, the Topics listed on our website. Its objectives are to provide a high-level forum for the dissemination and sharing of cutting-edge advances in engineering research and development, current primary research outputs, and significant accomplishments; to report progress in engineering science, to discuss trending topics, areas of interest, obstacles, and prospects in engineering development, and to take into account the well-being of people and the environment as well as engineering ethics; to promote engineering breakthroughs and innovations that benefit people and the environment.

Contents (Volume 2 & Issue 1 – 2025)

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025,
DOI: https://doi.org/10.48112/jestt.v2i1.15

Review

Cyberbullying in Technological Age: A Review of Legal Laws

Muhammad Taimoor Khan[1]*, Layiba Bibi[1] and Sanaullah[2]

[1]Abdul Wali khan university, Mardan, Pakistan

[2]Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Pakistan

* Corresponding Email: taimoor.usafxi007@gmail.com (M. T. Khan)

Received: 02 January 2025 / Revised: 01 February 2025 / Accepted: 07 February 2025 / Published online: - 28 February 2025

ABSTRACT

Cyberbullying is a harsh reality for many young people today, with the rise of technology making it easier for hurtful behaviour to spread. It has become a persuasive issue, with severe consequences. These consequences can be devastating, affecting not only their mental health but also, in the most tragic cases, leading to suicidal thoughts. Despite our best efforts to create a safe space online, we still have a lot to learn about how to protect our children from this kind of abuse and create a safer digital environment having a legal framework. Cyberbullying is a growing concern in Pakistan, but efforts to combat it are hindered by outdated and inadequate laws. The Electronic Transaction Ordinance 2002 and Prevention of Electronic Crimes Act 2016 failed comprehensively due to many challenges. This article delves into cybercrime legislation, including past acts such as the Electronic Transaction Ordinance 2002 and the Prevention of Electronic Crimes Act 2016. This article also discusses the latest amendments made in 2025 to the ETO. However, a glaring gap remains: the lack of a clear definition of bullying. Moreover, complexities surrounding intent, surveillance, awareness, jurisdiction, technology, and the age of criminal responsibility further complicate the issue. This article explores these challenges and discusses the need for comprehensive and effective legislation to protect Pakistan's citizens from the devastating effects of cyberbullying.

Keywords*:* Cyberbullying; Technology; ETO Amendment; Legislation

1. Introduction

We're living in a world where technology has changed everything. It's opened doors to new ways of learning and connecting. But, just like with any powerful tool, it comes with its own set of challenges. We're facing new kinds of threats, like cybercrime, and social conflicts that can arise online (Srivastava, 2012). The word "bully" has been a part of our language for nearly 500, years dating back to the 1530s (Donegan, 2012). At its core, bullying is a hurtful dynamic between two people: the one harming, and the one being hurt. The bully uses physical, verbal, or other forms of abuse to feel more powerful and in control. This can happen in obvious ways, like hitting or insulting someone to their face, or in more suitable ways, like spreading rumours or gossip (Donegan, 2012). Sadly, bullying has long been a painful reality for kids, often seen as a normal part of growing up (Limber & small, 2003). But that's changed in the last 20 years. People have started to question this view, realizing that bullying needs to be taken seriously and addressed (McCarthy, 2001). The world has finally taken notice of cyberbullying, and it's about time (Campbell, 2005). Many of us have experienced bullying firsthand, whether in childhood, adolescence or even as adults. Traditional bullying is a repeated, intentional act of aggression, carried out by one person or a group, targeting someone who can't easily defend themselves (Whitney & Smith, 1993; Catalano et al., 2014). Bullying is a form of abuse that thrives on an imbalance of power. At its core, it's a deliberate and repeated misuse of power to harm or intimidate others (Sharp et al., 2002; Rigby, 2002).

In recent years, bullying has evolved into a new form: Cyberbullying. This type of harassment involves using the Internet, social media, and electronic devices to intentionally intimidate, threaten and harm others. Cyberbullies exploit power and imbalances to repeatedly torment their victims through methods like texting, emailing, and video messaging (Juvonen & Gross, 2008; Marczak & Coyne, 2010; Patchin & Hinduja, 2015; Smith et al., 2008). Alarmingly, bullying is a widespread issue among children. In the UK alone, the NSPCC reported that over 25,000 counselling sessions were needed and just one year to support kids affected by

face-to-face and online bullying (NSPCC, 2015). Shockingly, some people have even viewed bullying as a form of entertainment or a normal part of growing up (Smith et al., 2008; Sabella, Patchin & Hinduja 2023). The reality is that bullying has severe and lasting psychological effects on both the bully and the victim. Research has consistently shown that face-to-face bullying and cyberbullying can lead to serious emotional and psychological harm. Studies have found that young people who are bullied in person often experience a range of negative outcomes (Beran & Li, 2007). Research has also revealed links between face-to-face bullying and a range of serious health issues, including psychiatric problems, psychosomatic complaints, and physical health concerns (Arseneault et al., 2006; Kim et al., 2006; Pozzoli, 2009). Cyberbullying also has devastating effects, leading to depression (Baker & Tanrikulu, 2010), stress, loneliness, anxiety, and low self-esteem (Katzer et al., 2009; Ybarra et al., 2006). In severe cases, it can even drive victims to suicidal thoughts (Katsumata et al., 2008) and, tragically, suicide itself (Feinberg & Robey, 2008).

Gaps: Despite growing awareness of cyberbullying, a significant research gap remains. First, there is a lack of empirical studies analyzing the long-term psychological impact of cyberbullying, particularly in the Pakistani context. Most existing research focuses on immediate effects, leaving the long-term consequences underexplored. Second, legal ambiguity persists regarding cyberbullying definitions and enforcement, necessitating comparative studies between Pakistan and other jurisdictions with established frameworks. Third, the role of artificial intelligence and automated detection in identifying and preventing cyberbullying remains an emerging yet underdeveloped field. Last but not least more research is needed on the effectiveness of intervention programs, including school-based awareness initiatives and psychological support systems for victims.

2. Cyberbullying

While technology has revolutionized our lives, offering numerous benefits and education, career, and social connections, it also has a darker side. The rise of online harassment, stalking, and bullying has made cyberbullying a pressing concern in today's digital landscape (Walrave & Heirman, 2011). The pervasive use of technology has given rise to a persistent and growing issue: Cyberbullying. This form of harassment may soon eclipse traditional bullying. Cyberbullying involves intentional, aggressive, and repeated behaviour intended to harass, intimidate, and threaten victims through digital means, often leveraging an imbalance of power (Juvonen & Gross, 2008; Marczak & Coyne, 2010; Patchin & Hinduja, 2012; Smith et al, 2008). Cyberbullying has a broader reach and greater persistence online, enabling multiple perpetrators to harass victims over time (Grigg, 2010). The anonymity of the internet and ease of access to victim's contact information make it easier for bullies to commit acts without facing consequences (Poland, 2010). Research suggests that cyberbullying often builds upon existing face-to-face bullying dynamics (Vandebosch & Van-Cleemput, 2008). Studies have found that most cyberbullying is perpetrated by individuals who already bully in person, targeting the same victims within their social networks (Juvonen & Gross, 2008; Ybarra & Mitchell, 2004). This overlap highlights the connection between online and offline bullying behaviours.

2.1. Types of Cyberbullying

Just like traditional bullying, cyberbullying comes in many forms, including;

- Flaming
- Harassment
- Impersonation
- Outing and trickery
- Exclusion and ostracism
- Denigration,
- Defamation
- Cyberstalking

Understanding cyberbullying requires recognizing the various forms it can take and the roles individuals play and each incident. By identifying and distinguishing between different types of cyberbullying, we can better comprehend the complexity and severity of this issue (El Asam & Samara, 2016; Feinberg & Robey, 2009; Gillespie, 2006; Kowalski, et al., 2012; Pearce, Cross, Monks, Waters, & Falconer, 2011).

Flaming involves exchanging hostile or aggressive emails or online messages, often with insults or profanity (Friedman & Curral, 2003). According to Turnage (2007), "flames" are defined as messages containing aggressive, hostile, or insulting content, often marked by hurtful messages filled with capital letters, excessive punctuation, and filthy obscenity. Flaming is often interchangeable with the term ***Trolling***, as both describe the act of intentionally posting hurtful or provocative content online.

Harassment is a form of cyberbullying that involves sending repeated, intentional, and upsetting emails to a person, often using offensive language (Feinberg & Robey, 2009; Wolak, et al., 2007).

Impersonation *is* a devastating form of cyberbullying where someone pretends to be another person often to deceive or harm others through fake online interactions (Kowalsky, 2009). The internet's anonymity allows individuals to easily create fake identities, often on social media, and pretend to be someone else. A tragic example is the case of 13-year-old Megan Meier, who took her own life after being bullied online by a woman using a fake identity (Tresniowaki, Truesdell, & Morrissey, 2008).

The ***outing*** is when someone shares private or embarrassing info about you online without your okay, which can be super hurtful and violating (Willard, 2007). Trickery happens when someone shares personal or embarrassing info with you, gaining your trust, but then betraying that trust by sharing it with others without your consent. Exclusion and ostracism are forms of cyberbullying where someone is intentionally left out of online groups, like games, chats, or social media groups, making them feel isolated and unwanted (Siegle, 2010; Willard, 2007; Kowalski, 2009).

Cyberstalking is another form of cyberbullying that involves tracking someone online, often without their knowledge or consent. This can include sending bullying messages, monitoring their activities, or even using other forms of cyberbullying tactics (Willard, 2007).

2.2. A technological evolution

The rise of technology has led to a proliferation of bullying particularly among youth. The advent of the internet and chat rooms in the 1990s created a breeding ground for online harassment (Subramanyam and Greenfield 2008). The widespread adoption of mobile phones among youth in the 1990s and early 2000s further facilitated bullying. By 2004 nearly half of 12 to 17-year-olds owned cell phones which increased to 75% later on (Lenhart 2010). Notably a Pew Research Center study found that 1/3 of teens send approximately 3,000 text messages per month (Lenhart 2010).

While parents may be certain that cell phones offer a sense of protection and security for their children they can also act as a tool for cyberbullying (Lenhart 2010). The rise of social media starting

with MySpace has created new platforms for interaction but also vulnerabilities for cyberbullying social media's ability to share personal information and create alias profiles can facilitate synonymous and hurtful interactions (Subramanyam and Greenfield 2008). Sites like Facebook Google and anonymous blogging platforms have enabled cyberbullying with severe cases including verbal abuse and targeted harassment (Subramanyam and Greenfield 2008). The propagation of technology has created new challenges for addressing bullying as technology continues to evolve. It is essential to develop strategies for preventing and addressing cyberbullying.

2.3. Prevalence and Risk Factors

A 2014 UK child line report revealed alarming cyber bullying statistics with 69% of 12 to 22-year-olds affected and 20% experiencing extreme cases. Facebook was identified as a major platform for bullying with 4500 young people seeking help in 2012-13. Almost half of parents (47%) lie awake at night worrying that their child will be bullied online (childline 2013). Research on cyberbullying prevalence has yielded varying rates making it challenging to determine an accurate measure. (Sabella et al., 2013). Most studies suggest that cyberbullying is less ubiquitous than in-person bullying (Sticca et al., 2013). On the other hand, a significant concern is that cyberbullying often goes unreported, with victims mostly keeping it to themselves, often suffering in silence (Smith & Slonje, 2008). Variability in prevalence rates exists with Gross and Juvonen (2008) finding that a staggering 72% of people surveyed had been cyberbullied, while a slightly higher 77% had experienced in-person bullying. Interestingly, Schneider et al. (2012) study revealed a different picture 15.8% of participants had faced cyberbullying while 25.9% had dealt with in-person bullying. These varying results are likely due to differences in research approaches (Sabella et al., 2013). Several reasons contribute to the underreporting of cyberbullying. Many victims feel that adults just don't get it and are powerless to stop the bullying, leading them to suffer in silence (Smith et al., 2008). Some victims may also carry the weight of responsibility feeling it's up to them to put an end to the bullying. Others may fear that adults won't take them seriously or believe their stories, leaving them feeling hopeless and alone (Campbell 2005; DCSF 2007). Additionally, victims may worry that reporting the incident would restrict their internet or device use (Campbell 2005; Juvonen and Gross 2008; Campbell et al., 2010). Studies have also identified demographic patterns in cyberbullying. Girls are more likely to report cyberbullying than boys (Schneider et al., 2012; Juvonen and Gross 2008). Sadly, cyberbullying is a growing problem among secondary school teens, who have easier access to technology, leaving them more vulnerable to online harassment (Campbell et al., 2012). Cyber stems from a toxic mix of emotions like shame, pride, anger, prejudice, religion and guilt (Jones and Manstead and Livingston, 2011).

2.4. Behavioral and Mental Health Consequences

Cyberbullying has severe adverse consequences on individuals affecting their security (Smith et al., 2008) well-being (Dehue et al., 2008) and causing trauma (Sourander et al., 2010). It should be addressed as a mental health issue rather than a discipline problem (Bauman et al., 2013). Research on cyberbullying effects was limited until 2005 relying on traditional bullying studies (Campbell et al., 2005). Tragic cases of teen suicides linked to cyberbullying have shed light on the devastating impact it can have (Agaston, Kowalski, & Limber, 2007; Baker and Tanrikulu 2010). Cyberbullying has been linked to serious health issues including stress, depression, loneliness, anxiety, and low self-esteem (Beshak, 2009). Psychological issues have also been reported along with the rise of despair (Juvonen & Gross, 2008), physical signs (Nearly & Joseph, 1994; Roland, 2002), eroding self-esteem, damaging academic performance and disrupting school life (Feinberg & Robey, 2008). The physical distance between the bully and the victim reduces social inhibition (Davies and Lee, 2008; Vandebosch et al., 2012). Cyberbullying is an adaptation of traditional bullying, highlighting the need for protective measures. Schools must raise awareness, adopt bullying policies, and teach online safety (Samara and Smith, 2008). While schools cannot prevent bullying entirely, they can encourage reporting and take disciplinary action.

3. Cyberbullying and the Law

Cyberbullying has severe psychological consequences, but its legal status remains unclear. Shockingly despite the UK's rising awareness about bullying, there's still no concrete law to protect victims, with tragic cases highlighting the need for change. For instance, Joshua Unsworth's case emphasizes the urgency for legal reform (Tozer, 2013). Another heartbreaking case is that of Daniel Perry, a 17-year-old who lost his life to bullying in 2013 after being tricked into creating an explicit video on Skype and later blackmailed online where anonymous users urged him to kill himself (BBC, 2014a). Daniel Perry's family urged Prime Minister David Cameron to take action and make the internet a safer place. Similarly, Ronan Hughes, a 17-year-old from Northern Ireland, committed suicide in 2015 after being tricked into posting online images and later blackmailed on Skype (The Telegraph, 2015). Although there is no specific law criminalizing bullying, whether offline or online, cyberbullying prosecutions can be applied under several legislative provisions. It is essential to note that all UK schools are required by law to have an anti-bullying policy addressing bullying and cyberbullying against pupils and teachers (Smith et al., 2012).

3.1. Cyberbullying and Cybercrime in Pakistan

The advent of 4G and 5G technologies has ushered in a digital revolution enabling rapid global communication. However, the increased digitalization and automation have left to a proportional right in cyber-crimes, and cyber-bullying cyber security ventures predict that cyber-crime will cost the world 10.5 trillion anyway by 2025. Pakistan has also seen an 83% increase in cyber crime or the past 3 years with the federal investigation agency FIA receiving over 102000 complaints.

3.2. Cybercrime Laws in Pakistan

Cybercrime laws in Pakistan have been passed by the Parliament.

- **Electronic Transactions Ordinance (ETO) 2002**

The Electronic Transactions Ordinance (ETO), enacted in 2002, was Pakistan's first IT-related legislation, ensuring legal sanctity and security for the local e-commerce sector. A major portion of Pakistan's cybercrime legislation was influenced by foreign cybercrime legislation, divided into 43 categories addressing various cyber offences. Pakistan's cybercrime law covers eight major aspects of the e-commerce industry, including recognition of electronic documents, electronic communications, digital signature regimes, website certification, stamp duty, attestation, jurisdiction, and offences.

- **Prevention of Electronic Crimes or Cybercrimes Ordinance 2007**

The Prevention of Electronic Crimes or cyber-crime Ordinance PECO was passed in 2007 covering electronic offenses such as terrorism damage to data electronic theory forgery authorized entry cyber stalking and cyber spamming cyber criminals in Pakistan may face sanctions ranging from 6 months in prison to the death penalty depending on the crime.

- **Prevention of Electronic Crimes Act 2016**

The Prevention of Electronic Crimes Act PECA was passed in 2016 providing a comprehensive framework for all forms of cybercrime It deals with internet crimes such as unauthorized data access denial of service attacks electronic forgery and cyber terrorism Becca imposes punishments on cyber criminals including imprisonment and fines for offences such as authorized access to key information systems disruption of important information systems involvement in terrorism-related offences importing or exporting electronic equipment for offensive use and data breaches. (Anees, 2025).

3.3. PECA Penalties on Cybercrimes

- Unauthorized access to key information system: up to 3 years imprisonment a fine of PKR 1 million or both.
- Disrupting important information systems with misleading motives: up to 7 years imprisonment and a PKR 10 million fine or both
- Involvement in terrorism-related offences: up to 7 years imprisonment a PKR 10 million fine or both
- Importing exporting or distributing electronic equipment for offensive use: up to 6 months imprisonment and a PKR 50,000 fine or both.
- Enrollment in data breaches: up to 3 years imprisonment a PKR 5 million fine or both including an intentional release of personal information online (Anees 2005).

4. PECA 2025

The Prevention of Electronic Crimes Amendment Bill 2025 recently passed by Pakistan's National Assembly introduces significant changes to the original PECA 2016 law. The key amendments are;

1. **Definition in the criminalization of fake news**: A new section 26A has been added to define and penalize the intentional spread of false information that may cause public fear panic or unrest offenders can face up to 3 years in prison a fine of up to 2 million PKR or both.
2. **Establishment of regulatory bodies:** Social media protection and regulatory authority: This authority will oversee social media platforms ensuring user rights and compliance with national laws it has the power to block or remove content deemed harmful offensive or country to Pakistan's ideology. **Social media complaints council:** A council has been formed to address grievances related to online content aiming to resolve cases within 90 days
3. **Mandatory registration for social media platforms:** Platforms are not required to register with the government and adhere to specific conditions content that insights violence promotes terrorism or contradicts national values can be removed
4. **Prohibition on broadcasting expunged parliamentary proceedings:** The bill prohibits the broadcasting or streaming of parliamentary proceedings that have been officially expunged.

These amendments represent a significant shift from the original Pet Car 2016 which primarily focused on cyber-crimes such as authorized access to information systems electronic fraud and cyberstalking The 2025 amendments expand the scope to include stricter regulations on online content, particularly concerning misinformation and content deemed harmful to national interest than the introduction of these changes has parked debate with concerns about potential impacts on freedom of expression in the broad powers granted to regulatory authorities critics argue that terms like fake news are vaguely defined and could be used to suppress descent supporters however is that the amendments are necessary to convert the spread of harmful content and misinformation online.

5. Conclusion

Cyberbullying is a persuasive and complex issue affecting individuals worldwide. It remains a critical issue, particularly among children and adult sense. The rise of technology and social media has transformed the way people interact creating new avenues for billing and harassment. This review highlights the severity of cyberbullying and its various forms and its devastating consequences on mental health. Despite the growing trend of cyberbullying, there is a lack of clarity surrounding its legal status emphasizing the need for comprehensive laws and policies to address this issue. Although laws like the ETO Act 2016 provide a foundation, they lack clarity and comprehensive enforcement mechanisms. Furthermore, this review underscores the importance of raising awareness promoting online safety and supporting victims of cyberbullying ultimately a multifaceted approach is necessary to prevent cyberbullying in create a safer online environment.

Future research should focus on long-term psychological effects, AI-driven prevention methods, and cross-jurisdictional legal comparisons to develop robust solutions. Additionally, policymakers must work towards clearer legislative definitions and stronger enforcement to ensure victim protection. Raising awareness, promoting digital literacy, and implementing school-based intervention programs are essential in combating this growing issue. A multidisciplinary approach encompassing psychology, law and technology is crucial to creating a safer digital environment.

References

ABC News. (2007). Parents: Cyberbullying led to teen's suicide. http://abcnews.go.com/GMA/story?id=3882520&page=1

Agatston, P. W., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyber bullying. Journal of Adolescent Health, 41(6), S59-S60. https://doi.org/10.1016/j.jadohealth.2007.09.003

Anees, M. (2025, January 16). A guide to cybercrime law in Pakistan. Graana.com. https://www.graana.com/blog/cybercrime-law-in-pakistan/

Arseneault, L., Milne, B. J., Taylor, A., Adams, F., Delgado, K., Caspi, A., & Moffitt, T. E. (2008). Being bullied as an environmentally mediated contributing factor to children's internalizing problems. Archives of Pediatrics & Adolescent Medicine, 162(2), 145. https://doi.org/10.1001/archpediatrics.2007.53

Baker, Ö. E., & Tanrıkulu, İ. (2010). Psychological consequences of cyber bullying experiences among Turkish secondary school children. Procedia – Social and Behavioral Sciences, 2(2), 2771-2776. https://doi.org/10.1016/j.sbspro.2010.03.413

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. Journal of Adolescence, 36(2), 341-350. https://doi.org/10.1016/j.adolescence.2012.12.001

BBC News. (2014). Daniel Perry's death sparks cyber-blackmail probe. https://www.bbc.co.uk/news/uk-scotland-24428437

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), 265-277. https://doi.org/10.2190/8yqm-b04h-pg4d-bllh

Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. The Journal of Student Wellbeing, 1(2), 16-33. https://doi.org/10.21913/jsw.v1i2.172

Calvete, E., Orue, I., Estévez, A., Villardón, L., & Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. Computers in Human Behavior, 26(5), 1128-1135. https://doi.org/10.1016/j.chb.2010.03.017

Campbell, M. A. (2005). Cyberbullying: An old problem in a new guise? Australian Journal of Guidance and Counselling, 15(1), 68-76. https://doi.org/10.1375/ajgc.15.1.68

Campbell, M., Cross, D., Spears, B., & Slee, p. (2010). Cyberbullying: Legal implications for schools. Centre for Strategic Education Occasional Papers, 118.

Catalano, R., JUNGER-TAS, J., MORITA, Y., OLWEUS, D., SLEE, P., & Smith, P. K. (2014). The nature of school bullying: A cross-national perspective. Routledge.

ChildLine. (2013). Childline annual review. NSPCC Learning. https://learning.nspcc.org.uk/research-resources/childline-annual-review
ChildLine. (2014). Childline annual review. NSPCC Learning. https://learning.nspcc.org.uk/research-resources/childline-annual-review.
Davies, M. R., & Lee, B. A. (2008). The legal implications of student use of social networking sites in the UK and US: Current concerns and lessons for the future. Education and the Law, 20(3), 259-288. https://doi.org/10.1080/09539960903262307
Dehue, F., Bolman, C., & Völlink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. CyberPsychology & Behavior, 11(2), 217-223. https://doi.org/10.1089/cpb.2007.0008
Department for Children, Schools & Families [DCSF]. (2007). Cyberbullying: A whole school community issue. https://old.digizen.org/downloads/cyberbullyingOverview.pdf
Didden, R., Scholte, R. H., Korzilius, H., De Moor, J. M., Vermeulen, A., O'Reilly, M., Lang, R., & Lancioni, G. E. (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. Developmental Neurorehabilitation, 12(3), 146-151. https://doi.org/10.1080/17518420902971356
Donegan, R. (2012). Bullying and cyberbullying: History, statistics, law, prevention and analysis. The Elon Journal of Undergraduate Research in Communications, 3(1), 33-42.
El Asam, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. Computers in Human Behavior, 65, 127-141. https://doi.org/10.1016/j.chb.2016.08.012
Feinberg, T., & Robey, N. (2008). Cyberbullying. Principal Leadership.
Feinberg, T., & Robey, N. (2009). Cyberbullying: Intervention and prevention strategies. National Association of School Psychologists, 38(4), 22-24.
Friedman, R. A., & Currall, S. C. (2003). Conflict escalation: Dispute exacerbating elements of E-mail communication. Human Relations, 56(11), 1325-1347. https://doi.org/10.1177/00187267035611003
Gillespie, A. A. (2006). Cyber-bullying and harassment of teenagers: The legal response. Journal of Social Welfare and Family Law, 28(2), 123-136. https://doi.org/10.1080/09649060600973772
Gillespie, A. A. (2006). Cyber-bullying and harassment of teenagers: The legal response. Journal of Social Welfare and Family Law, 28(2), 123-136. https://doi.org/10.1080/09649060600973772
Gini, G., & Pozzoli, T. (2009). Association between bullying and psychosomatic problems: A meta-analysis. Pediatrics, 123(3), 1059-1065. https://doi.org/10.1542/peds.2008-1215
Grigg, D. W. (2010). Cyber-aggression: Definition and concept of cyberbullying. Australian Journal of Guidance and Counselling, 20(2), 143-156. https://doi.org/10.1375/ajgc.20.2.143
Hoff, D. L., & Mitchell, S. N. (2009). Cyberbullying: Causes, effects, and remedies. Journal of Educational Administration, 47(5), 652-665. https://doi.org/10.1108/09578230910981107
Jones, S. E., Manstead, A. S., & Livingstone, A. G. (2011). Ganging up or sticking together? Group processes and children's responses to text-message bullying. British Journal of Psychology, 102(1), 71-96. https://doi.org/10.1348/000712610x502826
Juvonen, J., & Gross, E. F. (2008). Extending the school grounds?—Bullying experiences in cyberspace. Journal of School Health, 78(9), 496-505. https://doi.org/10.1111/j.1746-1561.2008.00335.x
Katsumata, Y., Matsumoto, T., Kitani, M., & Takeshima, T. (2008). Electronic media use and suicidal ideation in Japanese adolescents. Psychiatry and Clinical Neurosciences, 62(6), 744-746. https://doi.org/10.1111/j.1440-1819.2008.01880.x
Katzer, C., Fetchenhauer, D., & Belschak, F. (2009). Cyberbullying: Who are the victims? Journal of Media Psychology, 21(1), 25-36. https://doi.org/10.1027/1864-1105.21.1.25
Kim, Y. S., Leventhal, B. L., Koh, Y., Hubbard, A., & Boyce, W. T. (2006). School bullying and youth violence. Archives of General Psychiatry, 63(9), 1035. https://doi.org/10.1001/archpsyc.63.9.1035
Kowalski, R. M. (2009). Cyber bullying: Bullying in the digital age – By Robin M. Kowalski, Susan P. Limber and Patricia W. Agatston. Support for Learning, 24(4), 207-207. https://doi.org/10.1111/j.1467-9604.2009.01431_5.x
Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Reese, H. H. (2012). Chapter 14 cyber bullying among college students: Evidence from multiple domains of college life. Cutting-Edge Technologies in Higher Education, 293-321. https://doi.org/10.1108/s2044-9968(2012)0000005016
Lenhart, A. (2010). Teens, cell phones, and texting. Pew Internet & American Life Project. http://pewresearch.org/pubs/1572/teens-cell-phones-text-messages
Limber, S. P., & Small, M. A. (2003). State laws and policies to address bullying in schools. School Psychology Review, 32(3), 445-455. https://doi.org/10.1080/02796015.2003.12086211
Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). EU kids online II: A large-scale quantitative approach to the study of European children's use of the internet and online risks and safety. https://doi.org/10.4135/9781446273050145339 36
Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. Australian Journal of Guidance and Counselling, 20(2), 182-193. https://doi.org/10.1375/ajgc.20.2.182
McCarthy, P. (2001). Bullying: From backyard to boardroom.. Federation Press.
Mishna, F., Cook, C., Gadalla, T., Daciuk, J., & Solomon, S. (2010). Cyber bullying behaviors among middle and high school students. American Journal of Orthopsychiatry, 80(3), 362-374. https://doi.org/10.1111/j.1939-0025.2010.01040.x
Neary, A., & Joseph, S. (1994). Peer victimization and its relationship to self-concept and depression among schoolgirls. Personality and Individual Differences, 16(1), 183-186. https://doi.org/10.1016/0191-8869(94)90122-8
NSPCC. (2015, March). Always there when I need you: ChildLine review: what's affected children in April 2014. Criminal Injuries. https://www.criminal-injuries.co.uk/wp-content/uploads/2015/09/childline-annual-review-always-there-2014-2015.pdf
NSPCC Scotland. (2014). *NSPCC Scotland briefing on cyberbullying.
Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem*. Journal of School Health, 80(12), 614-621. https://doi.org/10.1111/j.1746-1561.2010.00548.x
Patchin, J. W., & Hinduja, S. (2015). Cyberbullying prevention and response, expert perspectives. Expert perspectives. Routledge, (33), 155-160. https://doi.org/10.4000/dse.850
Pearce, N., Cross, D., Monks, H., Waters, S., & Falconer, S. (2011). Current evidence of best practice in whole-school bullying intervention and its potential to inform cyberbullying interventions. Australian Journal of Guidance and Counselling, 21(1), 1-21. https://doi.org/10.1375/ajgc.21.1.1
Poland, S. (2001). Cyberbullying continues to challenge educators. District Administration, 46(5), 55. https://doi.org/10.2307/3385993
Quero, S. M., & Moralista, R. B. (2022). Coping with FB Cyberbullies: A Survey among College Students in the Philippines.
Rigby, K. (2002). How successful are anti-bullying programs for schools. In The Role Of Schools in Crime Prevention Conference.
Roland, E. (2002). Bullying, depressive symptoms and suicidal thoughts. Educational Research, 44(1), 55-67. https://doi.org/10.1080/00131880110107351
Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. Computers in Human Behavior, 29(6), 2703-2711. https://doi.org/10.1016/j.chb.2013.06.040
Samara, M., & Smith, P. K. (2008). How schools tackle bullying, and the use of whole school policies: Changes over the last decade. Educational Psychology, 28(6), 663-676. https://doi.org/10.1080/01443410802191910
Schneider, S. K., O'Donnell, L., Stueve, A., & Coulter, R. W. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. American Journal of Public Health, 102(1), 171-177. https://doi.org/10.2105/ajph.2011.300308
Sharp, S., Smith, P. K., & Smith, P. (2002). School bullying: Insights and perspectives. Routledge.
Shiels, M. (2003). A chat with the man behind mobiles. BBC News.
Siegle, D. (2010). Cyberbullying and sexting: Technology abuses of the 21st century. Gifted Child Today, 33(2), 14-65. https://doi.org/10.1177/107621751003300206
SLONJE, R., & SMITH, P. K. (2008). Cyberbullying: Another main type of bullying? Scandinavian Journal of Psychology, 49(2), 147-154. https://doi.org/10.1111/j.1467-9450.2007.00611.x
Smith, P. K., Kupferberg, A., Mora-Merchan, J. A., Samara, M., Bosley, S., & Osborn, R. (2012). A content analysis of school anti-bullying policies: A follow-up after six years. Educational Psychology in Practice, 28(1), 47-70. https://doi.org/10.1080/02667363.2011.639344
Smith, P. K., Smith, C., Osborn, R., & Samara, M. (2008). A content analysis of school anti-bullying policies: Progress and limitations. Educational Psychology in Practice, 24(1), 1-12. https://doi.org/10.1080/02667360701661165
Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., Ristkari, T., & Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents. Archives of General Psychiatry, 67(7), 720. https://doi.org/10.1001/archgenpsychiatry.2010.79
Srivastava, P. (2012). Educational informatics: An era in education. 2012 IEEE International Conference on Technology Enhanced Education (ICTEE), 1-10. https://doi.org/10.1109/ictee.2012.6208613
Sticca, F., Ruggieri, S., Alsaker, F., & Perren, S. (2013). Longitudinal risk factors for cyberbullying in adolescence. Journal of Community & Applied Social Psychology, 23(1), 52-67. https://doi.org/10.1002/casp.2136
Subrahmanyam, K., & Greenfield, P. (2008). Online communication and adolescent relationships. The Future of Children, 18(1), 119-146. https://doi.org/10.1353/foc.0.0006

The Telegraph Newspaper. (2015). Online trick 'led to teenage boy's suicide'. http://www.telegraph.co.uk/news/uknews/law-andorder/11661272/Online-trick-led-to-teenage-boys-suicide.html
Tozer, J. (2013, April 8). Schoolboy, 15, bullied to death by trolls on the internet: Friends say vile posts drove him to despair. Mail Online. https://www.dailymail.co.uk/news/article-2305332/Joshua-Unsworth-15-bullied-death-trolls-internet.html
Tresniowski, A., Truesdell, J., & Morrissey, S. (2008). A cyberbully conviction. People, 70(24), 73-74.
Turnage, A. K. (2007). Email flaming behaviors and organizational conflict. Journal of Computer-Mediated Communication, 13(1), 43-59. https://doi.org/10.1111/j.1083-6101.2007.00385.x
Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D., & Pabian, S. (2012). Police actions with regard to cyberbullying: The Belgian case. Psicothema, 24(4), 646-652..
Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. CyberPsychology & Behavior, 11(4), 499-503. https://doi.org/10.1089/cpb.2007.0042
Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. Children & Society, 25(1), 59-72. https://doi.org/10.1111/j.1099-0860.2009.00260.x
Whitney, I., & Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. Educational Research, 35(1), 3-25. https://doi.org/10.1080/0013188930350101
WILLARD, N. C. (2015). Cyberthreats Effectively Managing Internet Use Risks in Schools, 2007. Acesso em, 10.
Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. Journal of Adolescent Health, 41(6), S51-S58. https://doi.org/10.1016/j.jadohealth.2007.08.019
Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. Journal of Child Psychology and Psychiatry, 45(7), 1308-1316. https://doi.org/10.1111/j.1469-7610.2004.00328.x
Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associated distress related to internet harassment: Findings from the second youth internet safety survey. Pediatrics, 118(4), e1169-e1177. https://doi.org/10.1542/peds.2006-0815
https://www.yenisafak.com/en/world/explained-pakistans-controversial-peca-amendment-bill-2025-3-years-imprisonment-and-rs-2-million-fine-for-spreading-fake-news-3697641
https://runwaypakistan.com/breaking-down-the-peca-2025-and-digital-nation-bill-in-pakistan

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.14

Article

Monitoring Flood Waves Due to Overtopping: Case Study of Mosul Dam from Iraq

Mahmood.J.Alshammary[1*], Ibtisam R. Karim[1] and Mohamed Y.Fattah[1]

[1]Civil Engineering Department, University of Technology, Baghdad, Iraq

*Corresponding Email: bce.19.85@grad.uotechnology.edu.iq (M. J. Alshammary)

Received: 24 September 2024 / Revised: 13 January 2025 / Accepted: 15 February 2025 / Published online: 28 February 2025

ABSTRACT

When highlighting water resource exploitation and environmental management, interest in dam break hydraulics is growing due to the possibility of hydrological events brought on by climate change and the catastrophic dam breaches that often result in severe loss of life. Several areas are exposed to flooding risk due to flood waves resulting from dam failure. The current study aims to apply a numerical model that predicts the flood wave's characteristics due to a hypothetical overtopping failure in two dimensions. A numerical model (hydrologic engineering centre river analysis system 2D HEC-RAS) is implemented in this study. Mosul Dam, located on the Tigris River in Iraq, is utilized as a case study in this work. The 2D flow area was delineated on the digital elevation model to determine the inundation region and extracted n manning from a land cover layer connected with RAS MAPPER. The results explained that the maximum values of the depth and velocity in km 5 are 60 m and 10.10 m/sec, respectively. At the same moment, it is shown that maximum flood discharge happened near the dam body and that there is a roughly linear relationship between the flood flow and water surface elevation. The study concluded that the models are successful in analyzing the dam breaches by representing the variation of flood wave depth and velocity in two dimensions. Moreover, the ability of the Model to produce maps monitors the spread of hydrodynamic waves that indicate risk areas that are threatened by inundation, which aids in controlling the risks resulting from them.

Keywords*:* Mosul Dam; Flood Wave; Overtopping Risk; Two-dimensional HEC-RAS

1. Introduction

The dam breach hydraulics is a topic of interest in water resources, environmental protection, and other areas. Numerous significant losses of life and possessions have been due to hydrological events brought on by climate change that have caused dam failures. Accurate routing of the propagation of flood waves associated with dam breaks plays an important role in planning and economic considerations [1]. Overtopping happens when a huge amount of water comes from an upstream area that exceeds the dam crest [2]. While, 38% of dam failures, according to reports [3], were the result of overtopping due to insufficient spillway capacity. For example, Al Taiee and Rasheed,2009 [4] studied the hypothetical Mosul dam break in the upper Tigris River basin by utilizing the geographic information system and the simplified dam break model (SMPDBK). The main conclusions of this study helped Utilizing this data, pertinent public sector groups create strategic plans aimed at mitigating the impact of fatalities on nearby communities in the dam's downstream sections. Joshi et al 2017 [5] Investigated the risk of flood inundation due to a potential dam break that occurs in the Ujjani dam by employing- an unsteady analysis within the HEC-RAS model. Dam failure factors were predicted, and then maps of flood waves were produced in two dimensions. Finally, the study indicated that evaluating maps is crucial in preparing emergency action plans and flood disaster management.ÜNAL,2019 [6] applied the two-dimensional HEC-RAS model and GIS technique to analyze the catastrophe that occurred in Berdan Dam. The maps were obtained by the model, which denoted the flood distribution due to probabilistic breaches in two significant scenarios (piping and overtopping). Considering the arrival time of the flood, the highest (depths and velocities) of the waves are taken into account to prepare emergency plans created by public safety officials in the event of a probable flood on this scale. Kumar et al.2020 [7] analyzed the impact of the possible collapse of the southern Crete Island Bramianos dam on an area that lies downstream of the existing. The hydraulic analysis program HEC-RAS was used to calculate the estimated propagation of flood waves resulting from the dam breach. This study compared

instances from the DSM and DEM. It demonstrated how DSM details might more precisely depict surface relief and naturally occurring barriers like flora, structures, and greenhouses, allowing for more accurate hydraulic simulation results. Shahrim et al. 2020[8]compared one and two-dimensional models for the flood wave parameters due to the failures that occur in the Temenggor dam using HEC-RAS software. According to 1-D analysis, breach flow can reach 281588 m^3/s for pipe failure and 331030 m^3/s for overtopping failure. While, in the 2-D analyses, the flood discharge is 268,341 m^3/s in the pipe model and 328869 m^3/s in overtopping failure. The study deduced that the improvement of the inundation maps obtained from the 2-D model over a large area aids in preparing emergency action plans by illuminating the amount of flood hazard risk. Namara et al.,2021 [9] applied both HEC-RAS and HEC-GeoRAS models to produce maps that illustrated floods in the case of Awash Bello, upper Awash River basin, Ethiopia. The study concluded that the ability of the model to simulate the flood flow. Ge et al., 2021[10] examined the significant factors that impact life loss due to dam breaks. Based on interval analysis, it showed that social factors and hydrodynamic factors had a significant effect on live loss. Mhmood et al.2022[11] stimulated the flood parameters due to the virtual Haditha dam overtopping failure and the effect of these waves downstream the dam on the Euphrates River, Iraq, a long 124 km to Heet City. 1D HEC-RAS version 5.07 and ARC GIS were employed in this work. It concludes that the inundation maps obtained from numerical models contribute to preparing an emergency plan. Mohamed et al,2023 [12] highlighted the sensitivity analysis of soil properties and the size of the reservoirs on the dimension of the breach that potentially occurs in Mosul dam by using 2DHEC-RAS software.

The study concluded that soil properties and reservoir capacity had a greater effect on breach dimensions. Mohamed et al,2023[13] simulated the break in Mosul dam due to piping failure by the 2D HEC-RAS model. The study concluded that the two dimensions gave a good indication of the risk of the flood by producing a map that illustrated the distribution of the wave in two dimensions. Darji, K. et al,2024[14] Hydrodynamic modelling of dam breach floods for predicting downstream inundation scenarios using an integrated approach of satellite data, unmanned aerial vehicles (UAVs), and Google Earth Engine (GEE). This comprehensive research of hydrodynamic modelling in data-poor locations highlights the potential of sophisticated surveying and modelling approaches in flood assessment and management by assisting in the precise calculation of future likely flooding in downstream areas in the case of a dam breach. Regardless of the type of dam and how the breach forms within the dam body, a catastrophic dam failure causes uncontrollable and immense flooding downstream. The Hydrologic Engineering Center-River Analysis System HEC-RAS is a common method for simulating dam breaches. The chief aims of this research include the following: 1- An examination of the influence of a hypothetical overtopping case in Mosul dam using 2D HEC RAS version 6.2 and directing the flood wave's propagation within the Tigris River at a distance of about 225 km downstream the dam body .2- Producing maps of specific flood zones to assess the risk in the overall area in two dimensions.

2. Materials and methods

2.1. Description of study area

Mosul dam is deemed one of the largest earth dams constructed in 1985. It is 113 meters high and 3600 meters wide and is situated in the North of Iraq. It is constructed from zoned earth, filled with a mud core in the centre. The project serves multiple objectives, including flood control and water storage with a volume of 11.11 billion cubic meters at the highest operational level to generate electricity and utilize the reservoir for irrigation and tourism. The flood wave routing due to the hypothetical failure in Mosul dam is confined between the section of river that begins at Mosul dam and the downstream meeting point of the Tigris with the Great Zab River approximately 225km, in length, as illustrated in Figure 1 [15, 16]. Additionally, the hydraulic design specifications such as the maximum, normal and minimum water level and dimensions of the dam, etc. have been demonstrated in Figure 2 [17].

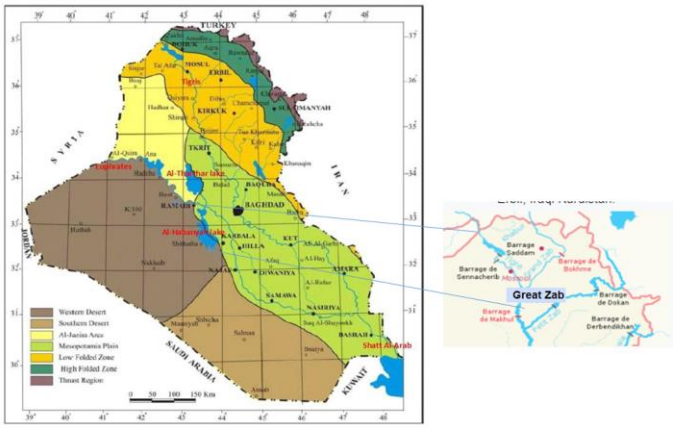

Figure 1: The position of the study area

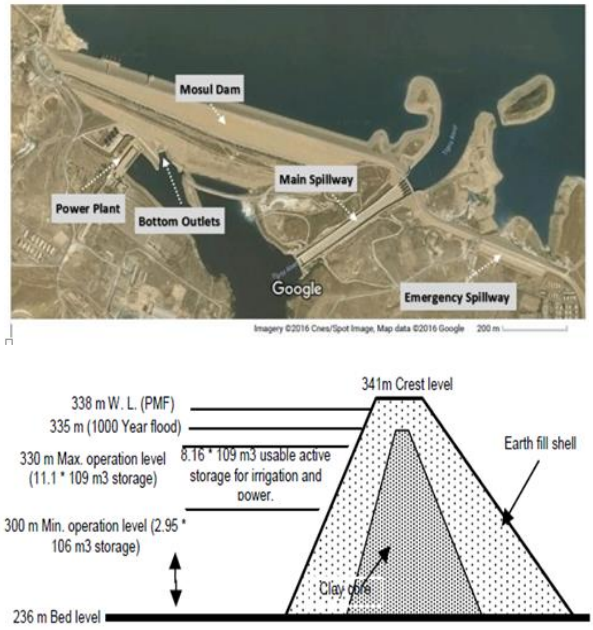

Figure 2: Layout of the Mosul dam: a). Image - satellite of Mosul dam and b). Typical profile

2.2. Digital Elevation Model

A wide range of fields and communities, including geomorphometry, hydrology, remote sensing, agriculture, cryosphere, defence, sport, land planning, natural hazards, and soil sciences, have adopted digital topography expressed as a Digital Elevation Model (DEM) [18]. The raster format that was allocated for the DEM, which potentially used with a GIS system[19]. Also, provides a basic representation of the 3D geometry of the Earth's surface. Which The Shuttle Radar Topography mission provided the Digital Elevation Model for the research region. Using a grid cell size of 14 m x 14 m that represented the topography level as shown in Figure 3 [20].

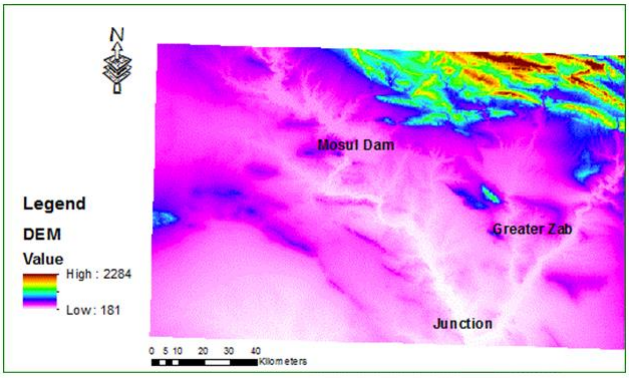

Figure 3: Digital Elevation Model of the study area

2.3. Land cover

The Landsat 8 satellite imagery, which has 3 bands with a spatial resolution of 30 m is used to represent the land cover map and is available on the website at [21]. The land cover map in Figure 4 has been treated in a GIS environment into supervised categories and then exported into HEC-RAS to determine the appropriate Manning's roughness coefficient values for each sort classified in the map, as indicated in Table 1. The roughness coefficient, is related to the entire land cover. Classes based on the HEC-RAS Hydraulic Reference Manual [22].

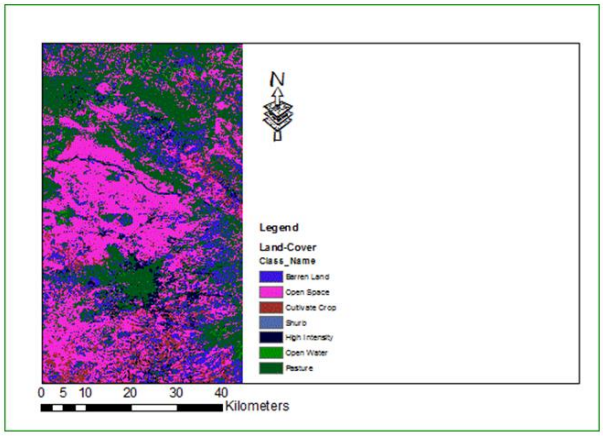

Figure 4: Land cover classification map.

Table 1:
The land covers types and parameter ranges.

Land Use Type	Pasture	Arable land	Vegetated river	Bushy grasslands	Urban area	Lakes	Clean river
Area (ha)	300	750	360	102	400.42	100.8	209
n Manning's	0.023-0.03	0.025-0.05	0.07-0.16	0.03-0.05	0.12-0.2	0.02-0.05	0.025-0.05

3. 2D HEC-RAS model

Version 6.2 of the Hydrologic Engineering Center United States' River Analysis System 2DHEC-RAS Army Engineers Corps has been extensively used to model and examine steady and erratic flow in natural and artificial open channels and sediment transport[23]. It comprises a user interface HEC-RAS MAPPER, discrete hydraulic analysis components, data storage, management capabilities, and graphics. The interaction of the data with the GIS software enhanced the ease of use of HEC-RAS in the dam failure simulation. In the 2D HEC-RAS software, the dynamic Shallow Water formula (SWEs) was applied. To route the flood propagation model that compounds Equations 2 and 3 as follows.

Equation (1), or the 2D diffusion wave equations (2) and (3) [24].

$$\frac{\partial H}{\partial t} + \frac{\partial (hu)}{\partial x} + \frac{\partial (hv)}{\partial y} + q = 0 \qquad (1)$$

$$\frac{\partial u}{\partial t} + \frac{u\,\partial u}{\partial x} + \frac{v\,\partial u}{\partial y} = -g\,\frac{\partial H}{\partial x} + vt\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2}\right) - C_f\,u + fv \qquad (2)$$

$$\frac{\partial v}{\partial t} + \frac{u\,\partial v}{\partial x} + \frac{v\,\partial v}{\partial y} = -g\,\frac{\partial H}{\partial x} + vt\left(\frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2}\right) - C_f v + fu \qquad (3)$$

Where: H: total height L, h: wave depth L, u *and* v : velocity components LT^{-1}, q : sink/ source flux L^2T^{-1}, g : acceleration,9.8 LT^{-2}, vt : (Eddy viscosity) $ML{-}1T\text{-}1$,Cf: Friction coefficient, and f**:** The parameter of Coriolis. The formation takes a trapezoidal shape to evaluate the breach parameters of fill dams. The width from the top, the width from the bottom, the gap, the depth, and the lateral slope are all geometric factors. Numerous empirical equations are developed for guessing the dam failure's breach factor and creation time [25]:

$$B_{avg} = 0.27\,K_o\,V_w^{0.32}\,H_b^{0.04} \qquad (4)$$

$$t_f = 0.0176\left(\frac{V_w}{g*H_b^2}\right)^{0.5} \qquad (5)$$

In which B_{avg}: breach width L, K_O : factor 1.3, V_w : the volume of reservoir over the bottom of the breach L^3, H_b: perpendicular distance from the peak dam to the breach reversal L, t_f: time T, g: gravity L/T^2.

4. 2D Simulation Model

The gathered data is deemed the main part of the methodology to simulate the dam failure using the 2D HEC-RAS model. It is divided into two categories: geography data, which gives a physical description of the case study (Digital Elevation Model (DEM) and Land Cover (LC) maps), and flow data, which provides information on the flow through dam characteristics like reservoir volume, dimensions, and probable maximum flood (PMF). Based on the irregular triangular network TIN obtained from a digital elevation model (DEM) with a 14m resolution after processing in RAS MAPPER, a hypothetical Mosul dam break is simulated and analyzed using the 2D HEC-RAS model. TIN is considered the main part of the 2D Model utilized for determining the 2D area flow downstream of the dam and Mosul Lake. Figure 5 shows the selection of the dimension of the cell applied to the 2D area of flow. The initial condition in the case of simulation is the flood risk or dam failures, which represent the distribution of water in the whole area before starting the simulation steps. The area elevation curve, the reservoirs of both dams and the depth of water in the Tigris River are considered the initial boundaries. Whereas, the reservoir outflow hydrograph and probable maximum flood (PMF) of the dam are deemed boundary conditions.

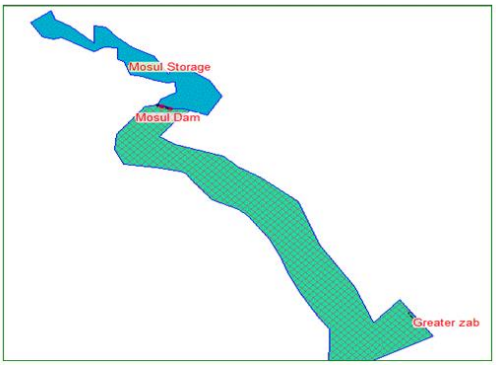

Figure 5: 2D Area flow connection.

5. Results

5.1. Result of breach failure

The Froehlich equation predicts that the overtopping failure occurs. (1:1) (H: V) is the side slope of the breach. At the same time, the top width of the break is 620 meters, and Figure 6 shows additional specific information about the dam breach

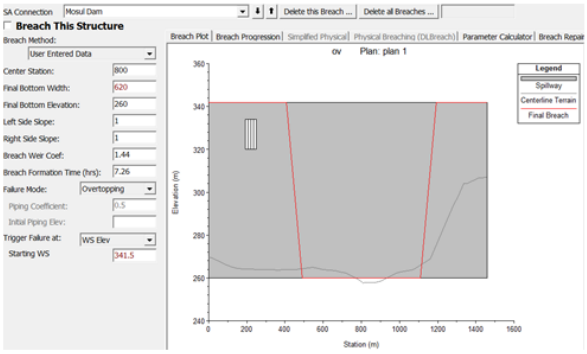

Figure 6: Section of breach parameter.

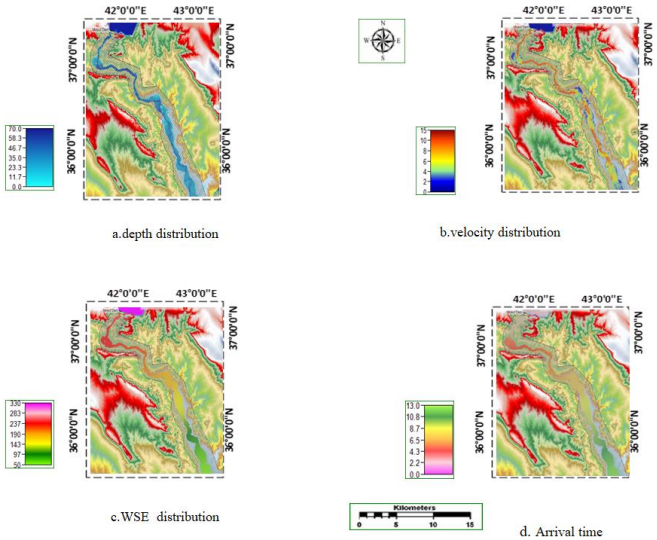

Figure 7: Dam break parameters distribution due to overtopping model.

5.2. Result of the Model of Hydrodynamics

Generally, the model conducts the dam break evaluations and monitors the flood routing at km 225 downstream of the Mosul dam. The initial level of the reservoir, which is 341.5 m, and the PMF for six hours at these moments are deemed initial and boundary conditions. Figures 7 (a-d) show the maximum water flow and water surface elevation within arrival time due to overtopping failure along the distance between Mosul dam and the point that meets between the Tigris River with Great Zab. The output maps that have been displayed on the digital elevation model with RAS-Mapper assistance can be utilized to model the flood wave that results from the overtopping breach. The depth varied from 20 m to 64 m at kilometer 5 from the dam body. While the velocity reaches 9.1m/sec near the dam body. It noted a high value of the flood discharge at km 17 approximately 300000m^3/s 5hr due to meandering. The values of WSE vary between 320 m neighbouring the body of the dam and then decrease with the flow direction due to energy losses to reach 200 m at km 225. The results of the studies are represented regarding the level of the water's surface, its depth, its velocity, and the time it takes for flooding to occur. The produced maps that illustrated the distribution of dam break parameters are illustrated in Figures 8 (a–d).

6. Discussions

A 2D HEC-RAS program was used in the current study to simulate the Mosul dam breaking, including mathematical relationships (Froehlich 2008), for the available dam break methods, the size of the breach, and the maximum dam break parameters. Then, it was noted that a breach occurred within 7.27 hours with a 1:1 side slope maximum width of 620 meters, as shown in Figure 6. While, the maximum depth is 60 m at km 5 downstream, south of the Mosul dam, and decreases slightly to the junction point between the Tigris River and the Great Zab to reach about 20m. Simultaneously, the outcomes illustrated that the maximum velocity value is 10.10 m/s at 5 km, decreasing slightly to reach 2.7m/s at km 225. Figure 7 illustrates the extent of the flood wave's dispersion along the river's two dimensions for arrival timings (5.1, 5.8, 6.8, 8.1, 11.8, 12.1) hr.

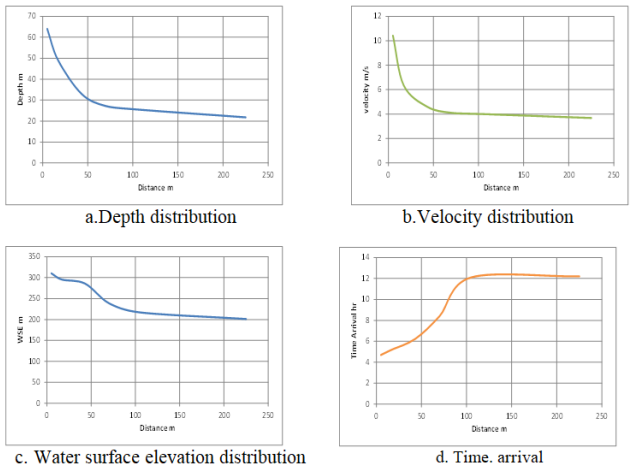

Figure 8: Relationship between the parameters of flood waves with distance.

The variations of depth, velocity, and water surface elevation are represented along the length of the Tigris River in Figure 8. Moreover, the maximum flow is 342939.2 m^3/s, and the corresponding WSE is 310.7 m. At the initial breach time, a reservoir's capacity is higher due to the overtopping failure due to meandering. While the slope of the WSE fluctuation due to enlargement or narrowing in the cross-section of the river. Figure 9 illustrates the relationship between water surface elevation and maximum flow. The highest value of the wave height results in the primary stages of the break.

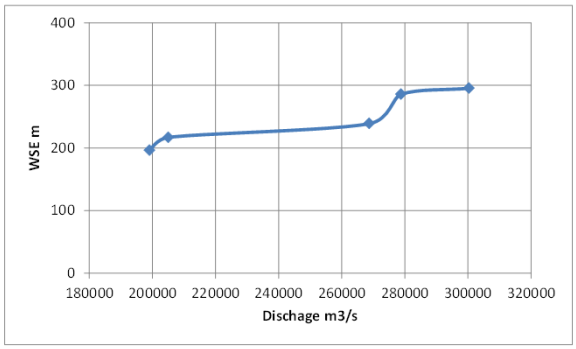

Figure 9: Relationship between stage and discharge due to overtopping failure.

7. Conclusion

The HEC-RAS model has successfully produced maps in two dimensions along the study area. The maps that were incorporated with the digital Terrine model represented the distribution of depths, velocities, and other parameters with the arrival time resulting from the phenomenon of overtopping failure. This analysis was able to estimate the period of creation of the Mosul dam breach, the direction of the flood wave propagation downstream, and provide a summary of the sequential events. The results have shown that maximum flood discharge happened near the dam body; moreover, high variations in depth, velocity, and flow values are due to overtopping failure. It noted a linear relationship approximately between the Water Surface Elevation and flood flow from upstream to downstream for the study area. The results explained that the maximum values of the depth and velocity in km 5 are 60 m and 10.10 m/sec, respectively. At the same moment, it is shown that maximum flood discharge happened near the dam body and that there is a roughly linear relationship between the flood flow and water surface elevation. Moreover, the maximum flow is 342939.2 m^3/s, and the corresponding WSE is 310.7 m. While the slope of the WSE fluctuation due to enlargement or narrowing in the cross-section of the river. Ultimately, this is one of the appropriate approaches to prepare for and avoid the risk due to flooded waves. Further studies should focus on methods for flood control to reduce catastrophic risk. By viewing the satellite images in the 2DHEC-RAS mapper, it is observed that there are median islands and bars along the Tigris River within the study area. Therefore, we recommend removing them and training the cross sections to pass the largest possible amount of flood flow.

Declaration

Acknowledgments: The authors thank the Ministry of Water Recourse in Iraq for providing the data.

Conflict of Interest: The authors state no conflict of interest

Data availability statement: Most datasets generated and analyzed in this study are in this submitted manuscript. The other datasets are available on reasonable request from the corresponding author with the attached information.

Statements and Declarations: We declare that the manuscript was done depending on the personal effort of the author, and there is no funding effort from any side or organization, as well as no conflict of interest with anyone related to the subject of the manuscript or any competing interest.

.

Reference

1. Amini, A., Arya, A., Eghbalzadeh, A., & Javan, M. (2017). Peak flood estimation under overtopping and piping conditions at Vahdat Dam, Kurdistan Iran. Arabian Journal of Geosciences, 10(6). https://doi.org/10.1007/s12517-017-2854.
2. Brunner G. W and CEIWR-HEC, "HEC-RAS River Analysis System User' s Manual," no. February, pp. 1–962, 2016.
3. Al-Taiee, T., & Mustafa, M. (2009). Hydrodynamic Simulation of Flood Due to Hypothetical Momentary Mosul Dam Failure. Tikrit Journal of Engineering Sciences, 27(4), 48–57. https://doi.org/10.25130/tjes.27.4.06.
4. ICOLD (International Commission on Large Dams). 1998 Dam-break Flood Analysis – Review and Recommendations. Bulletin 111. ICOLD, Paris.
5. Joshi, M. M., & Shahapure, S. S. (2017). Two-Dimensional Dam, Break Flow Study, Using HEC-RAS for Ujjani Dam. International Journal of Engineering and Technology, 9(4), 2923–2928. https://doi.org/10.21817/ijet/2017/v9i4/170904032.
6. Un, C. I." 2D Dam break analyses of Berdan Dam ". Master thesis, 2019, Civil Engineering Middle East Technical University, Turkey.
7. Kumar, N., Kumar, M., Sherring, A., Suryavanshi, S., Ahmad, A., & Lal, D. (2019). Applicability of HEC-RAS 2D and GFMS for flood extent mapping: a case study of Sangam area, Prayagraj, India. Modeling Earth Systems and Environment, 6(1), 397–405. https://doi.org/10.1007/s40808-019-00687-8.
8. Shahrim, M. F., & Ros, F. C. (2020). Dam Break Analysis of Temenggor Dam Using HEC-RAS. IOP Conference Series: Earth and Environmental Science, 479, 012041. https://doi.org/10.1088/1755-1315/479/1/012041.
9. Namara, W. G., Damisse, T. A., & Tufa, F. G. (2021). Application of HEC-RAS and HEC-GeoRAS model for Flood Inundation Mapping, the case of Awash Bello Flood Plain, Upper Awash River Basin, Oromiya Regional State, Ethiopia. Modeling Earth Systems and Environment. https://doi.org/10.1007/s40808-021-01166-9.
10. Ge, W., Wang, X., Li, Z., Zhang, H., Gelder, P. H. A. J. M. V., Wang, T., et al. 2021. Interval analysis of the loss of life caused by dam failure. J. Water Resour. Plan. Manag. 147, 04020098. doi:10.1061/(asce)wr.1943-5452.0001311.
11. Mhmood, H.H., Yilmaz, M., Sulaiman, S.O., 2022. Simulation of the flood wave caused by hypothetical failure of the Haditha Dam. J. Appl. Water Eng. Res. https://doi.org/10.1080/23249676.2022.2050312.
12. Mohamed, M., Karim, I., & Fattah, M. (2023). Impact of Dam Materials and Hydraulic Properties on Developing the Breaching Dimensions. Engineering and Technology Journal, 41(5), 716–723. https://doi.org/10.30684/etj.2023.138009.1368.
13. Mohamed, M. J., Karim, I. R., Fattah, M. Y., & Nadhir Al-Ansari. (2023). Modelling Flood Wave Propagation as a Result of Dam Piping Failure Using 2D-HEC-RAS. Civil Engineering Journal, 9(10), 2503–2515. https://doi.org/10.28991/cej-2023-09-10-010.
14. Darji, K., Patel, D., Prakash, I., & Hamad Ahmed Altuwaijri. (2024). Hydrodynamic modeling of dam breach floods for predicting downstream inundation scenarios using integrated approach of satellite data, unmanned aerial vehicles (UAVs), and Google Earth Engine (GEE). Applied Water Science, 14(9). https://doi.org/10.1007/s13201-024-02253-9.
15. Kh, T. S. Doctoral thesis, 2006."Mathematical Modeling of Hypothetical Failure of Multiple Dams- Mosul and Makhool Dams as a Case Study". Building and Construction Engineering Department, University of Technology, Iraq.
16. Ministry of Water Resource in Iraq. General Directorate of water resources management, hydrological studies center: Baghdad.1999.
17. Al-Ansari, N., Adamo, N., Knutsson, S., Laue, J., & Sissakian, V. (2020). Mosul Dam: Is it the Most Dangerous Dam in the World? Geotechnical and Geological Engineering, 38(5), 5179–5199. https://doi.org/10.1007/s10706-020-01355-w.
18. Guth, P. L., Adriaan van Niekerk, Carlos Henrique Grohmann, Muller, J.-P., Hawker, L., Florinsky, I. V., Gesch, D. B., Reuter, H., Herrera-Cruz, V., S. Riazanoff, López-Vázquez, C., Carabajal, C. C., Albinet, C., & Strobl, P. (2021). Digital Elevation Models: Terminology and Definitions. Remote Sensing, 13(18), 3581–3581. https://doi.org/10.3390/rs13183581.
19. Alwan,I., Karim,I., and Mohamed,M., 2018 "Sediment predictions in Wadi Al-Naft using soil water assessment tool," MATEC Web Conf., vol. 162, pp. 1–6, 2018, doi: 10.1051/matecconf/16203008.
20. Website metadata from satellite image http://glovis.usgs.gov
21. http:// livingatlas.arcgis.com › landcoverexplorer
22. Brunner, G. HEC-RAS River Analysis System: Hydraulic Reference Manual, Version 5.0.; US Army Corps of Engineers Hydrologic Engineering Center (HEC): Davis, CA, USA, 2016; pp. 1–538.
23. H. J. Khadim and H. O. Oleiwi, 2021, "Assessment of Water Quality in Tigris River of AL-Kut City, Iraq by Using GIS," E3S Web Conf., vol. 318, p. 04001, doi: 10.1051/e3sconf/202131804001.
24. Froehlich, D. C. (2008). Embankment Dam Breach Parameters and Their Uncertainties. Journal of Hydraulic Engineering. https://doi.org/10.1061/(asce)0733-9429(2008)134:12(1708).
25. I. R. Karim, Z. F. Hassan, H. H. Abdullah, and I. A. Alwan, 2021"2D-HEC-RAS Modeling of Flood Wave Propagation in a Semi-Arid Area Due to Dam Overtopping Failure," Civ. Eng. J., vol. 7, no. 9, pp. 1501–1514.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.13

Review

The Human Rights Implications of Scientific Progress: A Case Study on Gene Editing and Disability Rights

Anza Fatima[1], Aftab Haider[1*] and Asma Batool[2]

[1]Southwest University of Political Science and Law, China

[2]Government Girls Higher Secondary School, Kolo Tarar, Hafizabad, Pakistan

*Corresponding Email: aftabhaider@awkum.edu.pk (A. Haider)

Received: 02 January 2025 / Revised: 21 January 2025 / Accepted: 24 February 2025 / Published online: 28 February 2025

ABSTRACT

Gene editing tools like CRISPR-Cas9 hold great promise for treating genetic diseases but also raise important ethical concerns, especially regarding disability rights. While gene editing can eliminate inherited diseases, it could also worsen ableism and widen social divides by reinforcing discrimination against people with disabilities. This article will talk about the ethical challenges of gene editing, focusing on the impact on marginalized groups, such as the Deaf community, who see their conditions as part of their identity rather than something to be fixed. The research will focus on practical examples, like gene therapy for sickle cell disease and editing embryos for hearing impairments, and highlight the limited access to these technologies, which could deepen inequality. It calls for stronger global guidelines that include input from disability communities to prevent the technology from reinforcing social divisions. The results show that without clear limits, gene editing may lead to a society that values genetic traits over diversity and human dignity, urging policies that promote fairness and inclusion.

Keywords*:* Gene Editing; Human Rights; Disability Ethics; Genetic Discrimination; Bioethics and Regulation

1. Introduction

Throughout history, scientific advancements have profoundly shaped human society [1]. In modern history, each scientific breakthrough created advantages and problems for society. Scientists use CRISPR, and Cas9 effectively to make accurate changes to genes through their advanced DNA modification system [2]. CRISPR technology shows promise in treating genetic disorders through its ability to help patients with sickle cell anemia, cystic fibrosis, and some types of vision disorders. Powerful technologies always present potential dangers to their users. Misusing gene editing tools can harm human rights by favouring certain groups while neglecting others, especially people with disabilities. Human rights experts see gene editing as a contradictory process. Through gene-editing people with disabilities can enjoy better health by ending the pain from their specific diseases. The system may promote the idea that being normal is better than being disabled. Our approach to disability acceptance affects how society evaluates life value in the future. The use of gene editing methods leads to complex ethical and legal problems [3]. When parents choose to edit their child's genes, do the children have any power over this decision? Who gets to make choices about which disabilities and traits need change? Should countries control genetic technologies or should the business sector make its own decisions about these practices?

Our society needs a strong ethical and legal system to protect human dignity while safely advancing scientific research. Key objectives of this article are:

1. The scientific advancements in gene editing, particularly CRISPR, Cas9.
2. The human rights implications focus on disability rights, genetic discrimination, and consent.
3. Real-world case studies that illustrate both the promises and risks of gene editing.
4. Existing legal frameworks and the need for more inclusive regulations.

2. Scientific Progress and Gene Editing

Our readiness to face the possible outcomes becomes critical as we develop the ability to change human genetic material. A

basic gene editing technique lets scientists make exact DNA modifications to fix disease problems or insert beneficial qualities. The widely recognized tool CRISPR Cas9 functions as DNA scissors to edit specific gene locations [4]. Scientists now use prime and base editing techniques to make precise DNA changes by inserting single genetic letters without altering the DNA strand. Current scientific findings show we can stop inherited diseases from developing by making necessary changes to DNA before a child is even conceived. Scientists worry they may delete undesired traits if they can currently remove disease-related problems. Scientists agree that gene editing offers major benefits to medical research. Scientists can use this method to fix hereditary diseases and fight cancer yet make specific changes to genes while also building virus resistance. Through time, scientists have found new ways to use their research that were never intended before. Will gene editing remain a tool for disease prevention, or will it be used to create a "perfect" version of humanity? Parents could select a child's height intelligence and eye colour with this technology. Scientists compare genetic editing to other reproductive choices including IVF and genetic testing. There are concerns that genetic selection will create divisions between those who can afford genetic enhancements and those who cannot. When gene editing serves profits instead of ethical values it may deepen social disparities rather than fixing them. Organizations need to establish rules for who decides how gene editing will be applied. When doctors and scientists choose which genes to alter, does that imply they judge disabilities as defective organs for removal? Advocates for disability rights oppose genetic editing because they believe it reduces the value of disabled people and promotes beliefs that they should be modified instead of embraced. Take deafness as an example. Parents who have this genetic trait often select gene editing to improve their child's life. In the Deaf community, deafness forms their cultural heritage while they reject the notion that they should be cured. If society starts eliminating genetic conditions based on what is seen as “normal” or “better,” where do we draw the line?

3. Human Rights Concerns in Gene Editing

Technology provides impressive outcomes but creates tough moral dilemmas to solve [5]. Which groups will benefit from gene editing, and which will be excluded? Should we edit the genetic makeup of future populations when future people have no say in that decision? This critical issue drives the conversation among different stakeholders.

3.1. Right to Health vs. Right to Identity

Initial analysis shows that gene editing helps human rights by treating genetic illnesses while making people healthier [6]. Since medical experts can now treat cystic fibrosis and sickle cell anemia, why would anyone want to stop this progress? Doctors recognize this development as a significant improvement in healthcare. From an ethical and social viewpoint gene, editing technology creates comprehensive challenges. People with disabilities regard gene editing that removes their conditions as an attack on their fundamental sense of self. Many individuals do not view their disabilities as medical problems that require treatment. Members of the Deaf community identify deafness as their cultural background rather than an illness. When parents use gene editing to prevent deafness in their children, it raises the question of whether this intervention heals or erases an important aspect of the Deaf community. When people focus on creating better genes what will happen to people who currently live with a disability? They will encounter either more prejudice or need to explain why they exist. Disability rights advocates push social inclusion and better access over deleting disabilities because that is how they want to boost health.

3.2. Genetic Discrimination: A New Form of Inequality?

People with certain genetic traits might be treated unfairly because of this new form of discrimination. A future world will see enhanced genetic traits become financially exclusive to the wealthy class giving them permanent health, intelligence, and physical benefits over other people [7]. People with their original genes may experience diminished status compared to those who received genetic enhancements. Previous events demonstrate how harmful these beliefs proved to be. The concept of eugenics led people to enforce sterilization programs while discriminating against racial groups and performing genocidal actions to cleanse certain bloodlines. The techniques used to edit our genes might reactivate obsolete practices in a technologically advanced form. How might employers or health insurers respond when making decisions based on genetic traits? Laws like the Genetic Information Nondiscrimination Act currently help defend against genetic preferences but their strength will need to increase to protect people in an environment of routine genetic enhancement [8]. Without clear rules, the use of gene editing techniques may exacerbate social disparities rather than reduce them.

3.3. Consent and Future Generations: Who Owns Their DNA?

The issue of agreeing to genetic modifications creates strong disagreement among experts. The modifications made to an embryo's DNA will affect the whole life of a child who did not agree to these modifications. Researchers question whether people born through gene editing will later demand control over their genetics. People who support gene editing claim that when it helps decrease suffering it should be employed as a medical tool. Since parents make medical choices for their children to improve their health every day, they already determine their well-being. While gene editing changes DNA permanently having long-lasting effects on future generations. Our understanding of the long-term effects of gene removal may prove to be incorrect. How could the changed gene produce medical problems during the adult years? We cannot foresee the full consequences of such genetic changes. People wonder who should determine what qualifies as an undesirable genetic trait. Our present concern targets life-threatening medical issues but stakeholders will decide in the future which traits humans can edit. Where should we establish our boundaries regarding this genetic editing?

4. Case Studies: Gene Editing & Disability Rights

Real examples demonstrate how gene editing already changed our social practices [9]. Despite its life-saving medical potential, this technology generates strong moral questions about human rights. Which people obtain these medical treatments? Should medical science be permitted to eliminate specific impairments from our bodies? Will these advanced techniques remain limited to high-income groups or open for everyone to use? The real-life examples demonstrate that gene editing affects disability rights in multiple ways with both positive and negative results

4.1. Case Study 1: CRISPR Treatment for Sickle Cell Disease, a Medical Breakthrough, But for Whom?

Sickle cell disease creates debilitating health risks for African descent patients. Research shows that CRISPR-based gene therapy helps scientists fix the genetic problem behind this condition [10]. People celebrate this breakthrough as it marks the first practical solution to end a persistent medical challenge. Each patient who needs gene therapy treatment pays steep costs that reach hundreds of thousands of dollars. Most people who need treatment for sickle cell disease live in low-income areas without access to

high-quality medical care. Our efforts to cure sickle cell disease through medical treatment will create a new social imbalance when only rich people can access these treatments. These case forces us to determine if life-saving gene treatments should belong to everyone's basic human entitlement or remain confined to wealthy patient access only. The potential health divide might grow bigger when gene editing becomes available since disadvantaged individuals may still lack proper medical care.

4.2. Case Study 2: The Ethics of Editing Embryos for Deafness, Curing a Condition or Erasing an Identity?

When parents edit their child's genes to prevent deafness, they do it hoping for a better future. Many see this as a natural choice because they want their child to hear. Members of the Deaf community strongly oppose this approach, viewing it as a threat to their cultural identity. Deafness stands apart from other disabilities because its cultural traits create an identity through language and social bonds. Deaf people strongly oppose gene editing because they fear it tells society their way of life should not exist. Parents need to answer whether they should get to make decisions about which genetic traits are unacceptable in their offspring. The beginning of editing deafness suggests we can eliminate other undesirable physical traits. Do parents today plan to pick their children's genes based on IQ levels and physical stature plus character traits? The case shows how gene editing presents a risk of treating people with disabilities as if they need curing instead of supporting their unique characteristics. As society permits more editing of disability-related genes how will it affect human diversity representation of disabled people and their right to self-identify?

4.3 Case Study 3: Global Disparities in Gene Editing, A Future Divided by Genetics.

The use of gene editing for human enhancement might increase the gap between wealthy and poor people. Wealthy families can choose genetic enhancements for their children, granting them better health and intelligence, which lower-income groups cannot access. People with altered genes could step above economic elites to gain control in education classrooms and work arenas. This issue extends beyond financial concerns, as it challenges fundamental ethical standards. Medical researchers have unfairly used Indigenous and marginalized populations for testing in history. Will people from these underserved communities influence technology companies when they handle gene-editing powers? Who holds the authority to define what DNA is important and what is detrimental? This example shows that we need to make sure gene editing becomes available to everyone instead of giving it solely to individuals of high status. Global participation in gene editing ethical reviews and universal access to technology can prevent the spread of genetic inequity.

5. Legal and Ethical Frameworks: Who Controls Gene Editing and Why It Matters

To prevent unethical applications of gene editing, scientists must establish strong ethical and legal frameworks that safeguard fundamental human rights [11]. Human rights laws at an international level protect people from having their dignity violated as science develops further. Major disability rights organizations at UNESCO and the UNCRPD support ethical gene editing by insisting that all procedure decisions must respect human dignity, create social equality, and prevent rights violations [12]. Under UNESCO's Human Genome Declaration, everyone has equal rights to their genetic makeup and people should not harm their basic human rights [13]. The statement did not create a law because countries can choose to follow or ignore its recommendations. The UNCRPD handles disabled individuals' rights differently by making them essential members of policy decisions [14]. Despite established policies, people with disabilities have limited involvement in discussions about gene editing although they will experience its effects more than others will. The lack of disabled community involvement in policy decisions creates doubt about the intent of gene editing to help people with disabilities or to get rid of disabilities to maintain a discriminatory mindset towards disability.

Many international regions handle gene editing differently through varying levels of legal control, which creates scattered worldwide regulations today. The United States lets scientists perform gene editing studies yet blocks genetic changes that can pass from one generation to the next. Private US biotech organizations are challenging current regulations by pushing experimental research that worries experts about ethical problems. British scientists may edit genes in embryos for scientific research under approved conditions but cannot use these methods for creating babies. The UK regulates gene editing to keep the technology within acceptable ethical limits. In China, the infamous case of *Dr He Jiankui*, who genetically edited twin embryos to make them resistant to HIV, exposed major loopholes in the country's regulatory framework [15]. The judge's decision to send *Dr He* to prison showed that some nations have become more willing to try controversial gene editing experiments even without proper restrictions. The European Union follows a strict policy by banning germline editing while permitting medical studies within strict conditions. The world lacks a single set of laws governing gene editing which permits countries to progress quickly or slow down their efforts. When one nation or company dominates genetic editing they create an unfair distribution of healthcare benefits and human improvement opportunities. When countries do not work together to set rules for gene editing it will make genetic enhancements available only to those who already have power.

The primary ethical challenge lies in which groups will determine policies for gene editing. Scientists and businesses dominate gene editing discussions, but they leave out disabled people, ethicists, and marginalized communities. Disability rights activists see gene editing as a tool that strengthens ableist views about fixing individuals who have disabilities. The lack of participation by disabled people in gene editing development increases the risk that rules will focus on removing impairments instead of building an accepting society for diverse abilities. As parents, they might remove certain genetic elements that can result in Down syndrome or neurodevelopmental conditions to enhance their child's life. The theory overlooks important social and cultural aspects of health conditions. Deaf community members consider deafness not an illness needing treatment but a cultural heritage with its language and customs. Medical enhancement policies need to consider the ethical risks that gene editing poses to specific human identities.

Gene editing needs international management to create fair and ethical medical solutions. Governments must work with disabled individuals and other marginalized groups to shape gene-editing technology since experts from corporate and government sectors dominate its current development. Making gene therapy available to all people equally protects us from building a system that lets money determine a person's life chances based on their social position. Individuals who can fund gene-editing treatment gain an unfair advantage that separates them from everyone else. International cooperation needs to create standards that balance edited genes with fair human rights treatment [16]. Lawmakers should create rules that help scientists make ethical decisions about gene editing while preventing these advances from harming social fairness through diversity maintenance.

Scientists must create updated rules and ethical standards to prevent gene editing technology from going wrong. When science

only cares about its wishes and money in gene editing, we will create systems that support current divisions instead of fixing them. Gene editing tools must follow ethical principles that include fairness and respect for diverse human groups besides achieving technical breakthroughs. Through united protection of human rights and inclusive practices, we can guide gene editing toward its purpose of making the world healthier.

6. Critical Analysis and Limitations of the Study

This article examines how gene editing affects Deaf people and individuals with disabilities but does not go into other related aspects. Deaf people see hearing loss as their cultural identity, which includes its own unique language expressions art, and events. When deafness gets fixed through gene, editing it destroys an entire social group that values signing as their cultural identity. Researchers study genetic elimination systems as new technology. People might someday edit genes to treat deafness and other disabilities yet view them as medical issues rather than human variations. The technique extends beyond medical practice to eliminate an entire culture. Our understanding of human experience would become less diverse when we remove traits people consider undesirable.

The article points out that genetic engineering technology creates unfair treatment between rich and poor countries. The article has limitations because it lacks an examination of how gene editing affects universal impartiality. Rich countries and individuals have exclusive access to expensive gene editing technology today. A future society will divide into groups based on their genetic luck when enhancements remain expensive. We must not see this as simply an economic issue because altering human genetic material creates a new type of market for body parts. When people use gene-editing methods to improve their intelligence or resistance against diseases, they may change themselves into marketable products [17]. Wealthy families can purchase high-quality genetic traits for their offspring yet ordinary people must use their natural genetic traits. The development of gene-based opportunities may establish differences between individuals whose life chances depend on their genetic code. This article explores how genetically enhanced people could dominate society, leaving others at a disadvantage.

The study discovers essential issues about consent relating to the genetic editing of embryos. Parents who pick genetic features for their babies begin to treat their offspring like custom-designed products. Our basic human identity faces important ethical challenges in such a situation. Our new concept studies Genetic Consumerism, which turns gene editing into a market-based service. Parents might look for genetics services while businesses supply desired traits to customers. Making this business model of genetics possible would create a society where people pursue specific genetic qualities excessively while treating human life as mere assets to trade.

The article mentions UNESCO and UNCRPD yet does not thoroughly examine why the international community cannot collaborate on gene editing policies. Multiple countries hold varying regulations about gene editing which leaves plenty of room for legal ambiguity. Multiple nations have separate rules about gene editing with certain countries permitting free use while others prohibit it. Countries that allow minimal gene editing restrictions create an open space for unethical companies and individuals to perform experimental work in those regions. This approach suggests that countries should implement genetic laws aligned with their cultural and ethical standards. Different nations will create separate standards for gene editing which could produce an unconnected network of rules across the globe.

Our ability to engineer life changes human nature and asks what it means to be human. Our technological influence over human evolution may eventually replace natural evolutionary processes. Our actions and discussions about modifying genes directly impact who we are as people and could affect our collective existence in deep ways. A concept of "Post-Human Ethics" would develop to address interactions between people machines and animals when distinctions fade between them. The process of gene editing may redefine how we understand human nature and produce beings that escape traditional human classification. Future studies should investigate how scientific developments change moral standards and examine the difference between making life naturally and making it through technology.

7. Conclusion

The important ethical consequences of gene editing along with laws and social concerns need proper consideration today. When we misuse genetic technology, it will create new gaps between rich and poor by giving advantages to rich families. Our priority with gene editing should be the enhancement of lives for all individuals rather than producing an ideal racial type. The focus should be on making life better without damaging individual diversity and human dignity. Our success depends on strong ethical standards, international cooperation, and policies that ensure all communities benefit from technology. Our main concern is not if we can edit genes but how we should perform genetic changes while supporting human rights and equal opportunities.

References

1. R. Richta, *Civilization at the crossroads: Social and human implications of the scientific and technological revolution (International Arts and sciences press): Social and human implications of the scientific and technological revolution*. Routledge, 2018.
2. Y. Ma, L. Zhang, and X. Huang, "Genome modification by CRISPR/Cas9," *FEBS J.*, vol. 281, no. 23, pp. 5186–5193, 2014.
3. K. E. Ormond *et al.*, "The clinical application of gene editing: ethical and social issues," *Per. Med.*, vol. 16, no. 4, pp. 337–350, 2019.
4. A. Eid and M. M. Mahfouz, "Genome editing: the road of CRISPR/Cas9 from bench to clinic," *Exp. Mol. Med.*, vol. 48, no. 10, pp. e265–e265, 2016.
5. A. Haider, "Application of the United Nation Convention against Transnational Organized Crime: An Analysis," *Available SSRN 4686710*, 2024.
6. B. S. Coller, "Ethics of human genome editing," *Annu. Rev. Med.*, vol. 70, no. 1, pp. 289–305, 2019.
7. A. Buchanan, *Better than human: the promise and perils of enhancing ourselves*. OUP USA, 2011.
8. J. L. Roberts, "The genetic information nondiscrimination act as an antidiscrimination law," *Notre Dame L. Rev.*, vol. 86, p. 597, 2011.
9. R. Lei and R. Qiu, "Ethical and regulatory issues in human gene editing: Chinese perspective," *Biotechnol. Appl. Biochem.*, vol. 67, no. 6, pp. 880–891, 2020.
10. R. Luthra, S. Kaur, and K. Bhandari, "Applications of CRISPR as a potential therapeutic," *Life Sci.*, vol. 284, p. 119908, 2021.
11. M. N. Karagyaur *et al.*, "Ethical and legal aspects of using genome editing technologies in medicine," *Современные технологии в медицине*, vol. 11, no. 3 (eng), pp. 117–132, 2019.
12. A. Conti, "Drawing the line: Disability, genetic intervention, and bioethics," *Laws*, vol. 6, no. 3, p. 9, 2017.
13. S. H. E. Harmon, "The Significance of UNESCO's Universal Declaration on the Human Genome & Human Rights," *SCRIPTed*, vol. 2, p. 20, 2005.
14. U. Gudelytė, J. Ruškus, and K. T. McCrea, "'Help me to decide': A study of human rights-based supported decision making with persons with intellectual disabilities.," *Am. J. Orthopsychiatry*, 2024.
15. H. T. Greely, "CRISPR babies: human germline genome editing in the 'He Jiankui affair,'" *J. Law Biosci.*, vol. 6, no. 1, pp. 111–183, 2019.
16. I. Karunarathna, T. Hapuarachchi, U. Ekanayake, and S. Gunathilake, "The ethics of genetic editing: Navigating the future of science," *Proc. Uva Clin. Res.*, 2024.
17. E. Borg and A. Policante, "The Gene Editing Business: Rent Extraction in the Biotech Industry," *Rev. Polit. Econ.*, pp. 1–36, 2024.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.12

Article

Exploring The Influence of Social Network Sites on Students' Academic Achievement: The Moderating Effect of Social Support

Layiba Bibi[1*], Jalwa Sufyan Hussain[1], Sanaullah[2] and Saddam ur Rahman[1]

[1]Abdul Wali Khan University Mardan, KPK, Pakistan

[2]Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology, Pakistan

*Corresponding Email: layibabibi@gmail.com (L. Bibi)

Received: 22 November 2024 / Revised: 17 January 2025 / Accepted: 23 February 2025 / Published online: 28 February 2025

ABSTRACT

The widespread use of social networking sites SNS among university students has raised deep concerns about their impact on the academic performance of students. This study examines the relationship between SNS usage, academic performance and social support among university students. A quantitative research approach was employed in a self-report questionnaire with data collected from 200 University students in Mardan Pakistan. The results showed a positive correlation between SNS usage and academic performance as well as between social support and academic performance. Regression analysis reveals that SNS usage is a significant predictor of academic performance. Mediation analysis showed that social support mediates the link between SNS usage and academic performance. The study reveals that the impact of social networking site usage on academic performance is dual varying according to the manner of usage. The study's results have highlighted important areas of concern for many stakeholders like educator policymakers and researchers highlighting the need to consider the role of social media and academic settings in developing strategies that promote responsible social media use among students.

Keywords*:* Social Networking Sites; Academic Performance; Social Support University Students; Quantitative Research

1. Introduction

Technological changes have always been regarded as a powerful source of evolution. Still, the emergence of the internet has disturbed almost all the facets of the private, social, and career existence of mankind (Bughin et al., 2011). From the simplest communication methods to managing large corporations and organizations, we are taking advantage of the facilities based on internet availability. The technological advancement achieved in internet applications is almost unimaginable (Rainie & Wellman, 2019). The internet has proven to be a valuable tool for connection and communication with a significant portion of users engaging with social networking and blogging sites. Approximately 2/3 of internet users visit these types of sites accounting for around 10% of total internet time and a substantial 65% of overall internet usage. (Amichai-Hamburger & Hayat, 2011).

Social networking sites have enabled millions of people to connect, and exchange information, knowledge, and culture (Hansen et al., 2010). Classmates. Com was launched in 1995 and was recognized as the first official Social Networking Site. The purpose of its creation was to allow students to be connected while in school or after their schooling is complete (Boyd & Ellison, 2007). Facebook, founded by Mark Zuckerberg in 2004, has become the most effective and popular social networking site (Alef, 2010). However, prolonged use of social networking sites can compromise academic success and hinder to learning process leading to wasteful and undescribed activities (Kuppuswamy & Narayan, 2010). On the other hand, social networking sites can also facilitate social relationships among students to discuss daily learning processes and various issues. Social networking sites have become an important part of people's lives, but their impact on education and learning must be carefully considered (Boyd, 2017; Tsatsou, 2016). Social networks can be beneficial for students' learning processes and academic performance, as they provide opportunities for connection and information sharing (Tinto, 1997). However, social networks can also be insecure for teenagers, and their popularity has led to concerns about improper behaviour, such as sharing personal information and engaging in online discussions that may compromise security (Trusov, Bucklin, & Pauwels, 2009). The US Congress has enacted legislation aimed at restricting young peo-

ple's access to social networking sites in schools and libraries highlighting concerns about their impact (Boyd & Ellison, 2007). As developed nations establish policies governing social media use it becomes essential to investigate whether these platforms hinder students' academic progress (Boyd & Ellison, 2007). This research aims to identify the specific aspects of social networking that influence students' academic life and learning recognizing their social media has become an integral part of daily life for students primarily used to stay updated on friend's activities. Research has shown that the majority of college students (over 90%) use social networking sites, with students spending around 30 minutes per day on these sites (Cain et al., 2009). The purpose of this study is to investigate the impact of social networking sites on student's academic life and learning processes, exploring whether these sites have a positive or negative effect.

1.1. Statement of the Problem

The widespread adoption of social networking sites among university students has raised concerns about the potential impact on their academic achievement. Despite the benefits of social networking, excessive use has been linked to decreased academic performance, increased distraction, and decreased motivation. The link between social networking site usage and academic achievement is multifaceted and the influence of social support as a moderating factor remains unclear. The influence of social networking site usage on university students' academic achievement, and the extent to which social support moderates this relationship, is a significant issue that warrants investigation.

1.2. Objectives

1. To investigate the association between social networking site usage and academic performance considering demographic factors.
2. To investigate the effects of social networking sites on the academic performance of students.

1.3. Research questions

1. How do demographic factors (gender, age, social influences, and education) influence students' academic achievement?"
2. In what way does the use of social networking sites impact the performance of the students?

1.4. Significance of the study

The current study will be useful for many institutions in establishing the impacts of social networking sites. The conclusion of the present research will be useful for the administrator and other public and private university authorities to control the students' social networking sites use in the academic context. Furthermore, the conclusion of this study will be useful for the Ministry of Information and Communication Technology to learn about the penalties of social networking among students and how one can take necessary measures to control it.

2. Literature Review

The rapid integration of social networking sites SNS into student's daily lives has led to extensive research on their impact on academic performance. However, the findings remain inconsistent necessitating a deeper critical analysis of existing studies. A study by Boyd and Ellison (2007) found that social networking sites have gained immense popularity, with 46.8 million to 68.8 million users. However, their study primarily focused on usage statistics rather than evaluating how SNS influences academic behaviours. While there are also concerns about underage users, as international law requires users to be at least 18 years old. Despite this, research by Lenhart (2007) showed that 41% of users under 13 and 61% of users between 14-17 years old are using social networking sites. The study of Lenhart (2007) also failed to account for how these platforms affect cognitive and academic development, leaving a gap in understanding the long-term consequences of SNS among students. Another survey by Russo et al. (2009) revealed that students are frequent users of social networking sites, with 47% of 12–17-year-olds, 69% of 18–21-year-olds, and 20% of adults using these sites, although only a small percentage use them for communication purposes (Russo et al., 2009). The emergence of Social Networking Sites (SNSs) has sparked debate and research on their effects on users. Studies have found that SNSs have both positive and negative impacts. However, excessive use of SNSs has been linked to various problems, including psychological, physical, interpersonal, and educational issues (Li Charlene & Bernoff, 2007).

Many students are spending more time on social networking activities than studying, which can negatively impact their academic performance. The relationship between SNS usage and academic performance has been widely debated. Some researchers argue that SNS negatively affects student's academic success due to distraction and time mismanagement. Research by Hawkins, (2010) found that students' activities are closely linked to grade differences. However, this study did not control for individual differences in self-regulation and study habits, raising concerns about the validity of its conclusion. A study by Nachbauer & Kyriakides (2019) revealed that Facebook use is inversely correlated with users' GPAs, with users having lower GPAs than non-users. However, surprisingly, 79% of Facebook users believed that their use of the site did not negatively impact their academic performance, indicating a lack of awareness about the effects of their social networking behaviour. The impact of social media on academic performance is a pressing concern. Conversely, other studies suggest that SNS can enhance learning and academic engagement. The research by Camus et al., (2016) suggests that excessive Facebook use can lead to decreased academic performance and lower grades as students navigate their educational journey it's essential to consider the factors that influence their success the internet is a powerful tool that can either facilitate or hinder the learning process/. However, these studies often assume that students engage with SNS in an academically productive manner, overlooking the potential for passive scrolling or engagement with non-educational content. Furthermore, they also failed to address individual differences in digital literacy, which can influence how students utilize SNS for academic purposes (Kennedy, 2020).

Social networking sites provide students with the virtual space to connect with peers potentially alleviating feelings of isolation according to Lenhart (2007) students can create a second life online by making new friends and connections however this can also lead to a false sense of security as students may believe their online interactions are private when they are not. Research reveals that social networking sites have both positive and negative effects on students on the one hand they can increase self-efficacy and social exclusion while decreasing face-to-face interaction Lenhart (2007). On the other hand, scholars like Bandura (1977) and Balsamo (1995) argue that social networking sites can help mitigate social exclusion and increase self-organization among students.

Some researchers like Tinto (1997) believe that social networking sites can provide a continuous learning community substituting for academic and social achievement in educational settings social networking sites can facilitate collaboration sense-making and engagement among students (Ellison et al., 2007; Lampe et al., 2008). However, these studies do not directly link social support to SNS usage, missing an opportunity to investigate whether online social interactions provide similar benefits as in-person support systems. Students have shown that social media can positively im-

pact student's participation in higher education improving commitment to coursework and enhancing connections with peers and instructors social networking websites also help students maintain relationships when they move to new physical groups facilitating collaboration on projects and assignments (Madge et al., 2009). Furthermore, research by (O'Sullivan et al., 2004) revealed that instructors with high online disclosure can increase student motivation reduce uncertainty, and foster a positive attitude towards the course and instructor.

The other limitation in the literature is the over-resilience of self-reported data. Many studies rely on student-reported SNS usage and academic performance, which are subject to social desirability bias and inaccurate recall. Objective measures, such as time-tracking software and official academic records, are seldom used, raising concerns about data reliability.

2.1. GAPS

Despite the growing body of research on social networking sites and academic performance several gaps remain in the literature. The first one is inconsistent findings on SNS impact existing studies present mixed results regarding the effects of SNS usage on academic performance. While some research suggests that excessive SNS use distracts students and reduces study time other studies highlight its potential for academic collaboration and knowledge sharing. The lack of consensus indicates the need for further investigation into the specific ways in which SNS usage influences learning outcomes. The other gap is the limited examination of social support as a moderator although social support has been studied as a key factor in academic success few studies have explored its role as a moderating variable in the relationship between SNS usage and academic performance understanding how social support influences. This relationship could provide deeper insights into how students balance their online social interactions with academic responsibilities. Last but not least is the lack of longitudinal studies, most research on the SNS and academic performance relies on cross-sectional data which limits the ability to establish casual relationships. Longitudinal studies tracking students' SNS usage over time would offer a clearer picture of its long-term impact on academic achievement. To address these gaps future studies should conduct longitudinal research, utilize objective data collection methods, and explore demographic and contextual variations and the role of digital literacy and self-regulation strategies. By filling these gaps future research can provide a more comprehensive understanding of the relationship between SNS usage, social support and academic performance.

2.2. Theoretical framework

The following Figure 1 represent the theoretical framework of this study.

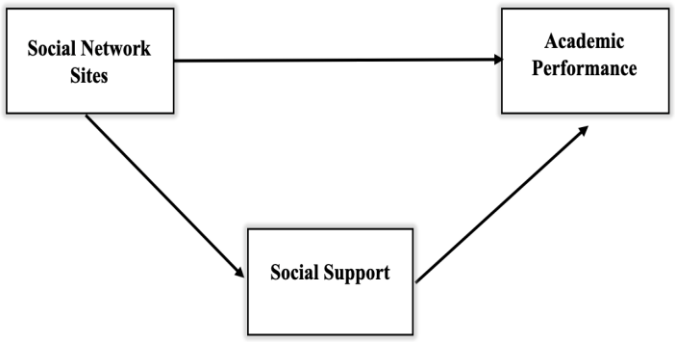

Figure 1: Theoretical Framework

2.3. Hypothesis

1. Using social networking sites is linked to improved academic achievement.
2. Social networking sites play a significant role in enhancing student's social connections and systems.
3. Social support is positively associated with students' academic performance
4. Social support will mediate the relationship b/w SNS and academic performance

3. Research Methodology

A quantitative research design was employed to gather and analyze data from a sample of 200 undergraduate students with an age range of 19 to 35 years. The purposive sampling method was utilized. The purposive sampling method was chosen because it enables researchers to select participants who meet specific criteria relevant to the study's objective. The other sampling methods were not feasible for some reasons such as logistical constraints and were unnecessary. The data was analyzed using SPSS 26 and assessed through statistical techniques. The findings were presented using means, standard deviations, and the Pearson Correlation Coefficient, Regression Analysis, and Mediation Analysis. A significance level of $p \leq .05$ was applied.

3.1. Measuring Instruments

To collect data student participants completed three questionnaires these questionnaires included a demographic form that gathered basic information about the student's social networking sites scale (SNS) (Kirschner & Karpinski, 2010), academic performance scale (APS) (Baisac, n.d.) and social support scale (Cohen et al., 1985).

3.2. Social Networking Sites Scale (SNS)

Developed by (Kirschner & Karpinski, 2010), this scale measured how often and for how long students used social networking sites. The questionnaire used Likert scale questions such as "How often do you use social networking sites" with responses ranging from strongly disagree to strongly agree.

3.3. Academic Performance Scale

Created by Carson this scale evaluated students' academic achievement performance the APS consisted of 8 Likert scale Christian such as "I made myself ready in all subjects" with responses ranging from strongly disagree to strongly agree the scale showed high internal consistency (.89) and test-retest reliability (.85).

3.4. Social Support Scale

Developed by Cohen et al., (1985) this scale assessed the pursuit of social support students received from family friends, and others The questionnaire used Likert scale questions such as "How often do you feel supported by your friends" with responses ranging from strongly disagree to strongly agree.

4. Results and Analysis

4.1. Demographic Information

The demographic table provides an overview of the 200 participants' characteristics, revealing a majority of males (74%) and participants aged 18-22 (86%), with most being unmarried (86%) and a small percentage being married (12%) or divorced (2%). The participants come from various academic departments, including Psychology (32%), Law (26%), Political Science (18%), Pakistan

Studies (6%), Sociology (9%), and International Relations (9%). These demographic characteristics provide context for understanding the diversity of the participants and may be useful in interpreting the results, particularly about the influence of demographic factors on academic achievement, as explored in Research Question 1.

Table 1:
Demographic Information of the Respondents

Demographic Information	Frequency	Percentage
Gender		
Male	147	74%
Female	53	26%
Age		
18-22	171	86%
23-27	28	14%
Marital Status		
Married	25	12%
Unmarried	171	86%
Divorced	4	2%
Department		
Psychology	63	32%
Political Science	36	18%
Law	53	26%
International relationship	18	9%
Sociology	18	9%
Pak studies	12	6%
Total	**250**	**100%**

***Note*: *f*=Frequency; %=Percentage; M=Mean; S.D.=Standard Deviation**

4.2. Descriptive Statistics and Correlation Analysis

Table 2 presents the descriptive statistics and correlation analysis of the variables, revealing that students spend an average of 18.36 hours on social networking sites (SNS), with an average academic performance (APS) score of 20.80, and an average social support (SS) score of 36.09. The correlation analysis reveals a weak positive relationship between SNS usage and APS ($r = 0.152$, $p < 0.05$), suggesting that moderate SNS engagement might support academic activities rather than hinder them. This could be due to students utilizing SNS for academic discussions, accessing educational resources, or engaging in peer learning. A weak positive relationship between SNS usage and SS ($r = 0.177$, $p < 0.001$), and a moderate positive relationship between SS and APS ($r = 0.304$, $p < 0.001$), indicating that higher SNS usage is positively correlated with better academic performance and greater social support, providing preliminary support for the study's hypotheses. These findings emphasized that SNS usage, when integrated with academic activities, may enhance student learning but excessive use for non-academic purposes could undermine academic performance. Additionally, the role of social support highlights the importance of maintaining strong peer and institutional support systems for students' success.

Table 2:
Descriptive statistics, Mean, Standard deviation (SD), and correlation of the variables

Variables	Mean	SD	1	2	3
SNS	18.3550	4.48436	1		
APS	20.7950	6.39197	.152*	1	
SS	36.0900	6.56256	.177**	.304**	1

Note: N=200 *p<0.05, **P <0.001

4.3. Regression Analysis

Table 3 Regression analysis: Regression analysis was conducted to determine the predictive power of SNS usage and social support on academic performance. These findings suggest that SNS usage significantly predicts academic performance ($b=0.152$, $p <0.05$), albeit with a small effect size ($R2 = 0.023$).

Social support is a strong predictor of academic performance ($b=0.0304$, $p < 0.001$), explaining 7.2% of the variance in academic achievement. This shows that students who perceive greater social support are more likely to perform well academically, possibly due to emotional encouragement, collaborative learning and academic guidance from peers and mentors.

Table 3:
List of Variable and Analysis

Variable	SS	AP
Constant		
SNS	.277***	.152*
SS		.304***
R2	.077	.023
Δ*R2*	.072	.018
F	16.486	4.711

N=200 *p<0.05, **P <0.001 ***p<0.0001

Regression analysis enables investigators to examine the connections between quantitative variables more comprehensively than simple correlation analysis does, and it can provide insights into the nature of predictor variables and their effects on outcomes. The practical significance of these findings suggests that educational institutions should foster online academic communities and peer support networks to maximize the benefits of SNS while minimizing potential distractions. Interventions such as digital literacy programs and structured online study groups could help students optimize SNS usage for academic success.

4.4. Mediation Analysis

Mediation analysis examines how the variable of interest influences outcomes through other variables or mediators, which can reveal more information about causal and sequential relationships. IV → MV → DV

The above mediation analysis explores the extent to which Social Networking Sites (IV) influence Academic Performance

(DV) through the mediating variable, Social Support (MV). Path 'a' depicts a direct, positive connection between Social Networking Sites (IV) and Social Support (MV) (β =. 406, p < 0. 001) which implies that the usage of SNS is positively related and leads to higher perceived social support among students. As seen in path 'b', Social Support (MV) has a positive and a moderate impact on Academic Performance (DV) (β =. 277, p < 0. 001) which signifies that a high level of social support leads to better academic performance. However, the direct impact of Social Networking Sites (IV) on Academic Performance (DV) (path 'c') is still significant (β =. 217, p < 0. 05), implying that SNS usage affects performance both directly and indirectly through social support. The last hypothesis, stating that IV Social Networking Sites have a significant indirect effect on DV Academic Performance through MV Social Support, was supported (β =. 112, p < 0. 05). This implies that although social support partly explains the association between SNS use and academics, there are other direct mechanisms by which SNS use impacts academic performance. This suggests that SNS contributes to academic success not only through direct engagement with learning materials but also by fostering social interactions that enhance student's academic motivation and well-being.

5. Discussion

The study employed a quantitative research approach which effectively examined the relationships between the variables a simple size of 200 participants was sufficient for conducting statistical analysis. The scales used to include the social networking sites scale academic performance scale and social support scale are well-established and reliable. The study limitations include the use of a non-probability sampling method and the lack of control or extraneous variables future studies should aim to recruit a more diverse sample use multiple measures of SNS usage and academic performance and control for extraneous variables to further understand the relationships between SNS usage academic performance and social support.

The correlation analysis reveals a positive relationship between social networking site (SNS) usage and academic performance (APS) ($r = 0.152$, $p< 0.05$). This suggests that students who spend more time using social networking sites tend to perform better academically additionally the correlation analysis showed a positive relationship between academic performance (APS) and social support (SS) ($r = 0.304$, $p < 0.0001$). This indicates that students who perform better academically tend to have higher levels of social support.

The regression analysis shows that SNS usage is a significant predictor of APS ($b = 0.277$, $p < 0.001$). This suggests that SNS usage is a significant factor in predicting academic performance The results also showed that social support is a significant predictor of APS this indicates that social support is also an important factor in predicting academic performance previous studies have also found a positive relationship between SNS usage and academic performance for example a steady by Kirschner and Karpinski (2010) found that students who used social networking sites more frequently tended to have higher GPAs another study by Junco (2012) founded students who used social networking sites more frequently tended to have better academic outcomes. Additionally, studies have found a positive relationship between social support and academic performance for example a study by Tinto (1997) found dead students who had higher levels of social support tended to have better academic outcomes another study by Purswell et al., (2008) found dead students who had higher levels of social support tend to have higher GPAs.

The study's findings support the theoretical framework which posits that SNS usage can have both positive and negative effects on academic performance depending on how it is used. The results also support previous studies that have found a positive relationship between SNS usage and academic performance as well as a positive relationship between social support and academic performance. The study results imply that educator policymakers and researchers highlight the need to consider the role of social media and academic settings and to develop strategies that promote responsible social media use among students' future studies should aim to recruit a more diverse sample and use multiple measures for SNS usage and academic performance and control for extraneous variables to further understand the relationship between SNS usage academic performance and social support.

6. Conclusion

This study explored the influence of social networking sites on students' academic achievement examining the moderating effect of social support the results showed a weak positive relationship between SNS usage and academic performance as well as a moderate positive relationship between social support and academic performance regression analysis revealed that SNS usage and social support or significant predictors of academic performance mediation analysis shows that social support partially mediated the relationship between SNS usage and academic performance. The findings support the theoretical framework and previous studies highlighting the importance of responsible SNS use and social support in promoting academic achievement. The study results have implications for educators' policymakers and researchers emphasizing the need to develop strategies that promote responsible SNS use and foster social support among students. Despite these insights, the study presents several limitations that future research should address. First, the reliance on self-reported data may introduce biases such as students may estimate or underestimate their SNS usage and academic performance. Future studies could incorporate objective measures such as academic records and digital tracking of SNS activity to improve data accuracy. Second this study focused on a specific university context limiting the generalizability of findings expanding research to include diverse educational settings disciplines and cultural backgrounds would provide a more comprehensive understanding of SNS. Effects on academic performance Future research should also explore the long-term impact of SNS usage on academic outcomes in longitudinal studies. Additionally investigating the role of digital literacy self-regulation and time management. Skills in moderating SNS effects could offer valuable insights into how students can use these platforms productively. Moreover, qualitative approaches such as in-depth interviews or focus groups could provide a richer understanding of students' experiences and motivations regarding SNS use in academic settings. By addressing these areas future research can contribute to the development of evidence-based policies and interventions that promote responsible SNS usage ensuring that students leverage these platforms as tools for academic and personal growth rather than sources of destruction.

References

Alef, D. (2010). Mark Zuckerberg: The face behind Facebook and social net-working. Titans of Fortune Publishing.

Amichai-Hamburger, Y., & Hayat, Z. (2011). The impact of the internet on the social lives of users: A representative sample from 13 countries. Computers in Human Behavior, 27(1), 585-589. https://doi.org/10.1016/j.chb.2010.10.009

Baisac, E. (n.d.). PDF academic performance questionnaire. Scribd. https://www.scribd.com/document/630722715/PDF-Academic-Performance-Questionnaire

Balsamo, A. (1995). Technologies of the gendered body: Reading cyborg women; Claudia Springer, electronic Eros: Bodies and Desire in the Postindus-

trial age; J. P. Telotte, replications: a robotic history of the science fiction film. Screen, 38(3), 296-301. https://doi.org/10.1093/screen/38.3.296
Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191-215. https://doi.org/10.1037//0033-295x.84.2.19
1Boyd, D. (2017). Why youth heart social network sites: The role of networked publics in teenage social life. https://doi.org/10.31219/osf.io/22hq2
Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x
Bughin, J., Corb, L., Manyika, J., Nottebohm, O., Chui, M., de Muller Barbat, B., & Said, R. (2011). The impact of Internet technologies: Search. High Tech Practice. McKinsey & Company.
Cain, J., Scott, D. R., & Akers, P. (2009). Pharmacy students' Facebook activity and opinions regarding accountability and E-professionalism. Amer-ican Journal of Pharmaceutical Education, 73(6), 104. https://doi.org/10.1016/s0002-9459(24)00112-8
Camus, M., Hurt, N. E., Larson, L. R., & Prevost, L. (2016). Facebook as an online teaching tool: Effects on student participation, learning, and overall course performance. College Teaching, 64(2), 84-94. https://doi.org/10.1080/87567555.2015.1099093
Cohen, S., Mermelstein, R., Kamarck, T., & Hoberman, H. M. (1985). Measuring the functional components of social support. Social Support: Theory, Research, and Applications, 73-94. https://doi.org/10.1007/978-94-009-5115-0_5
Ellison, N. B., Steinfield, C., & Lampe, C. (2006). Facebook-specific social capital scales. PsycTESTS Dataset. https://doi.org/10.1037/t53561-000
Hansen, D., Shneiderman, B., & Smith, M. A. (2010). Analyzing social media networks with NodeXL: Insights from a connected world. Morgan Kaufmann.
Hawkins, A. L. (2010). Relationship between undergraduate student activity and academic performance. https://doi.org/10.32597/honors/222/https://www.studocu.com/row/document/rivers-state-university-port-harcourt/child-psychology/pdf-academic-performance-questionnaire/67228268
Junco, R. (2012). Too much face and not enough books: The relationship be-tween multiple indices of Facebook use and academic performance. Computers in Human Behavior, 28(1), 187-198. https://doi.org/10.1016/j.chb.2011.08.026
Kirschner, P. A., & Karpinski, A. C. (2010). Facebook® and academic perfor-mance. Computers in Human Behavior, 26(6), 1237-1245. https://doi.org/10.1016/j.chb.2010.03.024
Kuppuswamy, S., & Narayan, P. B. (2010). The impact of social networking websites on the education of youth. International Journal of Virtual Communities and Social Networking, 2(1), 67-79. https://doi.org/10.4018/jvcsn.2010010105
Lampe, C., Ellison, N. B., & Steinfield, C. (2008). Changes in use and percep-tion of Facebook. Proceedings of the 2008 ACM conference on Computer supported cooperative work, 721-730. https://doi.org/10.1145/1460563.1460675
Lenhart, A. (2007). 'Teens, Privacy and Online Social Networks. How teens manage their online identities in the age of MySpace', Pew Internet & American Life Project Report. Privacy in the Information Society, 471-478. https://doi.org/10.4324/9781315246017-40
Li, Charlene, & Bernoff, J. (2007). Social technographics. Mapping Participa-tion In Activities Forms The Foundation Of A Social Strategy, 247-260. https://doi.org/10.5771/9783845263823-247
Madge, C., Meek, J., Wellens, J., & Hooley, T. (2009). Facebook, social inte-gration and informal learning at university: 'It is more for socializing and talking to friends about work than for actually doing work'. Learning, Media and Technology, 34(2), 141-155. https://doi.org/10.1080/17439880902923606
Nachbauer, M., & Kyriakides, L. (2019). A review and evaluation of approaches to measure equity in educational outcomes. School Effectiveness and School Improvement, 31(2), 306-331. https://doi.org/10.1080/09243453.2019.1672757
O'Sullivan, P. B., Hunt, S. K., & Lippert, L. R. (2004). Mediated immediacy. Journal of Language and Social Psychology, 23(4), 464-490. https://doi.org/10.1177/0261927x04269588
Purswell, K. E., Yazedjian, A., & Toews, M. L. (2008). Students' intentions and social support as predictors of self-reported academic behaviors: A comparison of first-and continuing-generation college students. Journal of College Student Retention: Research, Theory & Practice, 10(2), 191-206. https://doi.org/10.2190/cs.10.2.e
Rainie, L., & Wellman, B. (2019). The internet is in daily life. Society and the Internet, 27-42. https://doi.org/10.1093/oso/9780198843498.003.0002
Russo, A., Watkins, J., & Groundwater-Smith, S. (2009). The impact of social media on informal learning in museums. Educational Media Interna-tional, 46(2), 153-166. https://doi.org/10.1080/09523980902933532
Tinto, V. (1997). Classrooms as communities: Exploring the educational character of student persistence. The Journal of Higher Education, 68(6), 599-623. https://doi.org/10.1080/00221546.1997.11779003
Trusov, M., Bucklin, R. E., & Pauwels, K. (2009). Effects of word-of-mouth versus traditional marketing: Findings from an internet social networking site. Journal of Marketing, 73(5), 90-102. https://doi.org/10.1509/jmkg.73.5.90
Tsatsou, P. (2016). Internet studies: Past, present and future directions. Routledge.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.11

Article

Firewall Technology Testing in Pakistan: The Fine Line Between National Security and Freedom of Expression

Jalil Ahmad[1], Aftab Haider[1*] and Anisa khalid[2]

[1]Southwest University of Political Science and Law, China

[2]Aisha Public School and College, KPK, Pakistan

*Corresponding Email: aftabhaider@awkum.edu.pk (A. Haider)

Received: 02 December 2024 / Revised: 18 January 2025 / Accepted: 04 February 2025 / Published online: 28 February 2025

ABSTRACT

Concerns have been raised over the international trend of relying on firewall technology for cybersecurity and digital censorship, especially in Pakistan. Firewalls are important to protect critical infrastructure, but can also be used to restrict access to information as state-controlled devices. In this article, we critically examine Pakistan's firewall deployment, investigating whether it intended to promote national security or online freedom. This study applies qualitative analysis, through economic, legal, and technological assessment of firewall policies in Pakistan, especially in the light of the amendment of the Prevention of Electronic Crimes Act (PECA) in 2025, which was in the course of writing this article, and the implications of this on the economic, political and social life of the country. It also draws comparative insights from global cybersecurity models, including China and Iran, to analyze Pakistan's trajectory of digital governance. The key findings highlight that Pakistan's firewall policies have increasingly been used as a means of controlling the internet; laws are unclear and can be used to limit free speech and media. Firewall-based censorship also has hidden economic costs, which now reach $1.62 billion in 2024. Implications of this research suggest that digital rights and cybersecurity should be balanced in the policies. Key to preventing Pakistan's cybersecurity efforts from eroding democracy and economic growth is transparent firewall governance and independent judicial oversight. Without such reforms, Pakistan runs the risk of digital isolation, loss of investment, and online freedoms. The findings add to the ongoing debate about cybersecurity law, digital human rights, and technology in government.

Keywords*:* Firewall; Cybersecurity; Digital Rights; National Security; PECA 2025; Internet Censorship

1. Introduction

In past centuries, walls were constructed as shields against outside dangers, be it the Great Wall of China, which was constructed to prevent nomadic northern tribes from penetrating within, or the European castles, which were surrounded by high walls and moats to dismay robbers. The history and background of firewalls are examined to understand how they became widely deployed and how they can make organizations and household networks safer places [1]. Even the term "firewall" itself, is not very old. It originated in 1764 and was used to refer to structures that helped prevent fire from spreading to other buildings, steam-powered trains, etc. Firewalls were established as significant components of computer protection by the 1980s, even though they began as simple filtering devices on routers. In the modern world, there are advanced security systems that regulate traffic between networks according to set security standards [2]. The Next Generation Firewalls (NGFWs) have become an essential part of modern cybersecurity as they incorporate intrusion prevention, deep packet inspection, real-time threat intelligence, and cloud security [3]. This article will discuss the importance of firewall technology in Pakistan and how it is being experimented and implemented for its impacts on security and freedom of speech. It analyses the differences between cyber security and cyber censorship, evaluating whether the deployment of firewalls in Pakistan meets the country's security requirements or whether it is an attempt to regulate freedom of speech on the Internet. The key objectives that are covered in this article are as follows;

1. How firewalls protect against cyber threats, with a focus on Pakistan's digital security landscape.
2. Whether firewall testing in Pakistan is genuinely about cybersecurity or a means to restrict digital freedoms.

3. How firewall policies intersect with Pakistan's regulatory framework, including the Pakistan Electronic Crimes Act (PECA) 2016.

4. The financial and political costs of internet restrictions, and their impact on Pakistan's digital economy.

Through a thorough analysis of these objectives, this article will explore the dual role of firewalls as an important defence against cyber-attacks and a possible mechanism for the government's control over online expressions.

2. Role of Firewall in cyber security

When constructing the concept of a firewall with its historical development, it is impossible to overestimate its importance in modern cybersecurity [4]. Firewalls act as the primary barrier against cyber threats and prevent unauthorized access and unlawful activities on the network [5]. As the modes of cyber threats increase, today's firewalls have incorporated new functions like intrusion prevention, DPI, and threat intelligence in real-time. Such features not only recognize but also counteract threats that may emerge in the future. Among the new advances in the field of firewalls is the concept known as the next-generation firewall (NGFW). NGFWs enhance the features of traditional firewalls by integrating them with other security solutions such as application control, intrusion prevention, and cloud intelligence [6]. It enables the identification of threats more effectively and accurate prevention procedures that can respond to the challenges of the modern cyberspace environment flexibly.

2.1. National security perspective

From a national security perspective, firewalls perform an important function for a network as the first line of defence against cyber threats and unauthorized intrusions [7]. These are positioned as the first line of defence in a network and are constantly analyzing traffic and applying a set of pre-defined security rules to regulate the flow of incoming and outgoing traffic. Firewalls can effectively protect against complex attacks like DDoS attacks by blocking harmful traffic that tries to disrupt services [8]. They are also used to prevent such IP addresses from enjoying the loopholes in network services to gain access to sensitive configurations. Governments must protect sensitive information, like financial records, to keep taxpayers' data safe. They need to manage the risks related to information security effectively. Information security officers in the public sector face the ongoing challenge of limiting the damage from security breaches, protecting networks from threats, and ensuring the security of government systems. To meet these challenges, governments need to implement a sound logging and intrusion detection system and create network management frameworks that would secure internal and external risks. The Great Firewall of China, implemented in 2008, controls and censors the flow of data, making China one of the strictest countries in the world when it comes to internet freedom [9]. Even though it has been more than a decade and is still dynamic, the Great Firewall has been effectively preventing politically sensitive information and collective action. Nevertheless, it continues to enable the majority of Chinese Internet users to use social networks, entertainment, and some forms of news. On the other hand, the protests in Iran in the new millennium have depended a lot on the Internet for planning and information sharing. Banned Iranians have also relied on digital means to disseminate information to both international audiences as well as the internal Iranian population. However, the Iranian government knowing the dangers of the internet has come up with the National Information Network (NIN) [10]. The NIN aims to improve the interconnection and the management of communication domestically as well as internationally. It encapsulates the government's efforts to control information dissemination and still retain control over social media. North Korea has a very weak internet system, with Kwangmyong, the national intranet, available only to selected people. Nevertheless, North Korea has been actively promoting itself as a cyber-power on the level of such countries as the USA, China, Russia, Great Britain, Israel, and Iran. The country has ramped up its cyber capabilities, as seen by the Sony Pictures hack, the WannaCry attack, and the DarkSeoul attack, even though the government has denied its involvement in these incidents. Cybersecurity has been an issue of concern in the United States for many years, and cybercriminals have attacked different industries. From 2005 to 2015, the cyber security organization recorded over 12,000 cyber incidents, which included data security breaches and violations. By 2017, the U.S. Department of Defense (DoD) had to enhance its defences by using advanced firewalls to protect vital military data, this is due to the rising complexity of cyber threats [11]. In the same year, hackers targeted different systems by using different tools such as viruses, worms, Trojans, DoS, DDoS, ransomware, and SQL injection. These cyber exploits were put at $445 billion globally meaning that there is a need to step up the defence against cyber incidents [12]. Pakistan, like many other countries, has seen growth in online services and information technology in its organizations, thanks to support from higher authorities [13]. One of the leading driving forces in this regard is NADRA (National Database and Registration Authority) which is responsible for operating the centralized national identity database in Pakistan. This database is used in many sectors such as the banking sector, passport offices, the Election Commission, mobile companies, and even international agencies like the FBI. NADRA is the only organization that deals with the registration and collection of population data in the country [14]. Due to its enhanced level of technological adoption, NADRA has been named among the most efficient organizations in the world. A report by Threat Track Security (2014) revealed that NADRA is among the best organizations in terms of modern technologies for managing sensitive data. Similarly, the European countries have adopted the Security Content Automation Protocol (SCAP) algorithm for their National Vulnerability Database (NVD) [15]. This protocol makes vulnerability management, security measurement, and compliance to be automated, this is in line with the international trend of improved cybersecurity.

However, the issue of cybersecurity threats persists. Criminals have gone for the accounts, trying to steal personal details such as those belonging to institutions like NADRA. Such breaches have been witnessed by organizations such as Cybersecurity, Stanford, CA (USA) and Pro Pakistani (2013). Since NADRA holds very sensitive national data, it is possible that it could fall prey to cyber terrorism, which would aim at either incapacitating the services offered by NADRA, corrupting human confidential information, or using the data for other wrong purposes. Pakistan being a developing country is in the stage of integrating cyber services throughout different fields. With this development, the protection of information from third parties has become of paramount importance in organizations. One of the issues is the appearance of social sites as websites that allow users to freely communicate and share information with friends. However, these platforms have turned into the most vulnerable to cybercriminals who seek to get unauthorized access to users' data with their places of residence. With these platforms becoming more popular, it becomes important to keep user data safe from cyber criminals to retain consumer confidence and uphold personal privacy.

Pakistan has accepted the emerging real dangers of cybercrimes and has developed several institutional structures to support its cybersecurity programs. Among these are the Pakistan Computer Emergency Response Team (Pak CERT), the Pakistan Infor-

mation Security Association, and the Computer Emergency Response Team (PISA-CERT) [16]. These teams are part of a worldwide trend where CERTs (Computer Emergency Readiness Teams) and CSIRTs (Computer Security Incident Response Teams) are established in both the government and business to address cyber threats and manage cybersecurity. While CERTs and CSIRTs deal with cybersecurity problems, they are different in some aspects. CERT is a trademark term referring to the intelligence of cyber threats, people who identify, secure, prevent, and mitigate threats. CSIRT on the other hand is a cross-functional team that offers legal and technical remedy. CERTs are especially oriented to national threats affecting critical infrastructures, the economy, national security, and DoS attacks. Pakistan has created the 'Pakistan Research Centre' under the Senate Defense Committee's Cyber Security Task Force to improve its cybersecurity and protect its cyberspace. In the same year, May 2018 to be specific, Pakistan established the National Centre of Cyber Security (NCCS) at Air University Islamabad to improve the country's cybersecurity systems [17]. Further, to deal with technological abuse in Pakistan, the Federal Investigation Agency (FIA) framed the National Response Centre for Cyber Crime (NR3C) in 2007. NR3C provides services including network forensics, technical training, and handling of computers, videos, mobile, and many other cybercrimes [18].

Despite these efforts, NR3C still faces limitations in preventing cybercrimes and addressing cyber offences due to a lack of capacity. However, the legal framework of cybercrimes in Pakistan has been established in the Pakistan Electronic Crimes Act (PECA) 2016, and it also lacks a strategic approach towards cybersecurity and its enforcement is still in progress [13, 18]. Cyber security in Pakistan is gradually emerging as a critical problem due to rising threats of cyber-criminal activities, cyber warfare, and terrorist activities. These challenges pose a threat to national security given the fact that main infrastructures and governmental and private sectors are at high risk[4]. The weakness is caused by several factors: old hardware and software, lack of training, and unawareness of threats. To this, one can add the fact that modern terrorist organizations have started using the Internet to perform their crimes, which adds to the challenges facing the country's security forces [19]. The government has introduced several steps to counter these important issues like the formation of cybersecurity response teams and laws like the Pakistan Electronic Crimes Act (PECA). However, these efforts are still inadequate as the threats in cyberspace continue to surge. There is a high demand for a strong and effective cybersecurity system to protect national interests. The only sustainable way forward is for the public and the private sectors to work more closely together. This would ensure that resources, expertise, and intelligence could be shared effectively to deal with cyber threats. Moreover, international cooperation should be improved when it comes to creating measures that affect global cybercrimes [20, 21]. Pakistan also needs to invest in technologies that can identify and counter cyber threats before they occur. The formulation of a national cybersecurity strategy that will be on par with international standards will be a central factor in the attainment of long-term cybersecurity.

2.2. Freedom of Expression

In the past decade, predominantly in the last few years, the internet has emerged as a major source of disseminating information and fighting media restrictions imposed by the authorities. This expansion can be directly attributed to the ever-growing internet users around the world. There are over two billion unique internet users today, more than doubling in the past five years. This shows how important online communication has become. The Internet is now a major means by which people communicate, obtain information, socialize, and even transact business, and governments have sought ways and means of regulating and, in some instances, controlling this important medium [22, 23]. This shift in policy has taken many forms such as website blocking and content filtering, manipulation of content, cyber-attacks, and the harassment of bloggers many of whom have been imprisoned for their online activities.

3. Legal and Policy Framework in Pakistan

3.1. The Prevention of Electronic Crimes Act (PECA) 2016 and Its Impact on Internet Freedom in Pakistan

Most of the offline human activities have gone online due to information and communication technology, which has resulted in high usage of the internet, including Pakistan. The increasing rate of cybercrimes led Pakistan to pass the PECA 2016 to prevent malicious activities through the internet [24]. However, when compared to similar cybercrime legislation in other countries, people have pointed out that PECA has stricter penalties and contains provisions that outlaw activities that are not considered unlawful in other countries. PECA, effective from August 16, 2016, is one of the most debated laws in Pakistan, especially with freedom of speech. Many civil society groups, opposition parties, and international human rights organizations have criticized this as overly harsh, flawed, and problematic. The law has raised specific uncertainties over its effects on freedom of speech on the internet in Pakistan.

3.2. Sections 3 and 4: Vague Terminology and Due Process Issues

The new penalties are introduced in sections 3 and 4 of PECA for unauthorized access to data and information without proper permission. According to Section 3, any person who accesses data or information systems for a dishonest purpose is liable to imprisonment for a term that may extend to three months, or a fine that may extend to fifty thousand rupees or both. Section 4 also forbids copying or transmitting data without permission and prescribes imprisonment (up to 6 months) and/or a fine of up to one hundred thousand rupees [25]. However, these sections use terms like dishonest intention, information system, unauthorized access, and transmission of information, and that raises many issues about due process. That is why the law that defines crimes in rather vague terms can lead to a situation when the very right to free speech is limited. In the U.S., courts pay special attention to vague laws, especially those related to the First Amendment. The U.S. Supreme Court stated in Connally v. General Construction Co. that a law is unconstitutional if an average person cannot easily understand its meaning. Likewise, the vagueness of provisions in PECA can lead to denial of due process, which in turn affects freedom of speech and expression for civil society activists, opposition politicians, journalists, and the common person who uses social media.

3.3. Sections 11 and 37: Hate Speech and Content Removal

PECA also talks about hate speech and content removal provisions. Section 11 prescribes a maximum of seven years imprisonment and or a fine for anyone who circulates information on media that incites sectarianism, inter-faith, or racial [25]. Under section 37 of the law, access to published content can be restricted or blocked by authorities if it is necessary for the national security, public order, morality, or defence of Pakistan or if it is considered as 'offensive' under the PECA [26]. As in Sections 3 and 4, these provisions are also ambiguous, and such terms as 'dissemination of information," 'hatred' and 'public order' are vague. These sections are too broad and allow authorities to censor content without specific stipulations and engulf important concerns of censorship of

free speech. Lacking proper protection measures to prevent the elimination of the posted information, these provisions can become instruments of oppression in the hands of administrators and regulators, limiting the rights of the people to share their opinions on the Internet.

3.4. Effect on Democracy and Human Rights

The vagueness of PECA and its wide-ranging provisions are problematic for rights that form the very basis of civil liberties such as the right to free speech. Owing to the availability of ambiguous and broad terms within the law, those in support of democratic changes, free access to information, and human rights may be suppressed or punished. The law's adverse effect on freedom of speech and expression, freedom of information, and academic freedom threatens democracy and the promotion of human rights in Pakistan.

3.5. Financial Impact of Pakistan's Internet Restrictions

As Pakistan's government attempts to gain greater control over its cyber sphere through the new national internet firewall, this move is not without monetary implications. In 2024, Pakistan had the highest financial loss from internet restrictions at $1.62 billion, more than Sudan and Myanmar, which are in civil wars. Asia was the hardest-hit region, with major losses in Pakistan, Myanmar, Bangladesh, and India due to these restrictions. These four countries are among the six most affected nations in 2024 proving that internet censorship has profound economic impacts. The financial cost is a clear indication of the current and future economic implications of internet blackouts and restrictions to freedom of access to the internet.

4. Global Approaches to Regulating Online Content

Different countries have unclear definitions of illegal content, leading to various regulation approaches. The United States (US) and China can be viewed as the two extremes in terms of approach to the regulation of content shared online. While the US has relatively liberal policies that restrict freedom of speech on social media to a limited extent, China thoroughly regulates the usage of the internet. Between these two poles, there are such states and actors as India, the European Union, Great Britain, Germany, etc., each of which is designing its model of content regulation as the balance between freedom, security, and governance.

4.1. Basic Provisions of the ICCPR on Freedom of Speech

Article 19: Freedom of Expression

Article 19 affirms freedom of expression, which includes the freedom to obtain, receive, and impart information [26]. However, it also allows for restrictions, provided that:

1. Law provides such restrictions and it has to be ensured that the restriction is clear, easily understandable, and unambiguous so that it cannot be used arbitrarily against any person.
2. They aim at a legitimate interest of the state, for instance, national security, public order, public health, or morals.
3. They satisfy the necessity and proportionality test whereby the measures adopted are the least intrusive and are proportionate to the stated aims without unreasonably jeopardizing freedom of expression.

Article 20: Prohibition of Certain Forms of Expression

In contrast to Article 19, which permits certain limitations, Article 20 obligates states to prohibit specific forms of expression:

1. Promoting national, racial, or religious enmity leads to discrimination, hostility, or violence. This provision works in conjunction with Article 19 since it deals with expressions that are likely to incite violence and infringe on the dignity of individuals. However, there are still concerns about which direction the human rights protection is taking, nevertheless, the development of the rights in peace, security, and justice for all people in the world is the most powerful tool [27].

4.2 Freedom of Expression in States of Emergency (Article 4, ICCPR)

Article 4 of the ICCPR allows states to derogate from some rights, including freedom of expression, during a State of Emergency [27]. This is allowed only under specific conditions:

1. *Existence of a Public Emergency:* Some situations must indeed be about the nation's life.
2. *Strict Necessity:* This must be the case with the measures taken.
3. *Non-Discrimination:* These measures may not be based on race, colour, sex, language, religion, or social origin.
4. *Proportionality:* Derogations must be no wider in scope and no longer in duration than is necessary for the emergency.

The Siracusa principles also help to guide and ensure that derogations do not go beyond the bounds of necessity and do not become a pretext for trampling dissent and rights arbitrary.

4.2. Ensuring Balance: Safeguards and Mechanisms

Striking a balance between national security and freedom of expression requires:

1. *Legal Clarity:* Speech regulation laws must be narrowly drawn and should refer only to clear and present dangers of breach of the peace, and should not be overly broad or vague to suppress dissent.
2. *Independent Oversight:* Restrictions must be applied through mechanisms such as judicial review or independent monitoring bodies, which should ensure their application and prevent abuses.
3. *Proportionality Assessments:* Restrictions on expression must be the least intrusive means to address security concerns and proportionate to the threat posed, and states must prove that.
4. *Transparency and Accountability:* Transparency in decisions taken by governments should be provided, rationale for restrictions should be disclosed, and governments should engage with civil society to protect public trust.
5. *Regular Reviews and Sunset Clauses:* Periodic review is required of temporary restrictions, and in particular of those implemented in states of emergency, to be sure that they are proportionate and necessary. Restrictions can be sunsetted when the emergency has ended.

Guiding principles exist as to what a country would need to do when deploying surveillance technologies. The voluntary and non-legally binding principles seek to show how governments can meet their commitments to democratic values, human rights, and fundamental freedoms, as required under their international obligations and commitments. In three areas of concern, the principles are designed to guard against the misuse of surveillance technologies by governments and their agents. Still, in recent decades, technological progress has been progressing, especially due to the exponential growth of Internet connectivity, and the world has been receiving enormous benefits from it. If used responsibly and by international law, surveillance technologies are an important tool to protect national security, public safety, and critical infrastructure and facilitate criminal investigations [28, 29]. Similarly, conducting complex investigations calls for advanced technological equipment consisting of forensic software, advanced data analysis tools, and high-tech equipment [30, 31]. If a country lacks these technological resources, it may not be able to conduct investigations efficiently, which could make it less complicated for organized crime to thrive. These technologies go so far as to further ensure that people can

continue to exercise their rights and liberties. Surveillance technologies are used responsibly to improve safety and security while complying with the rule of law. As these technologies develop, governments must take steps to make sure these technologies are used lawfully and responsibly, and that they include appropriate information safeguards to regulate the collection, handling, and disclosure of information collected through their use. The effectiveness of these protections is essential to the protection of individual privacy, personal data, and human rights, and to promoting transparency, accountability, and civic participation, all while we continue to pursue legitimate objectives, including law enforcement, public safety, and national security.

The legislation defines and regulates a wide range of tools as *'surveillance technologies'*. These technologies include products or services that are used to detect, collect, exploit, intercept, monitor, preserve, process, analyze invasively observe, or retain sensitive data, personally identifiable information (including biometric data), and communications regarding individuals or [32, 33]. These technologies can, of course, be lawfully used, but the misuse of these technologies by governments remains a major concern. The guiding principles address how surveillance technologies are to be used in three particular areas of concern. It should be stressed that these principles are not to apply to activities not in these listed areas. Governments to unjustifiably interrupt freedom of expression, discourage human rights and fundamental freedoms, or enable technology-based gendered violence or discrimination, online or offline must not use surveillance technologies. They also must not perpetuate harmful or discriminatory norms or stereotypes, or undermine bodily autonomy by unlawful collection or misuse of personal health data, including reproductive and sexual data, or by the dissemination of intimate images. These guiding principles are a set of common practices and standards, with variations in implementation based on national legal frameworks and systems. Other nations may have more entrenched safeguards, indeed more robust safeguards that show even stronger commitments to these principles. In summary, it emphasizes the need for lawful and responsible use of surveillance technologies to avoid harm and uphold human rights and freedoms.

5. Critical Analysis

The recent amendment to the Prevention of Electronic Crimes Act (PECA) 2025, which was approved by the National Assembly while this article was being written, makes it even more important to analyze Pakistan's firewall technology and how it affects freedom of expression and national security. The amendment makes it a crime to share *false and fake information*, with penalties of up to three years in prison and fines. This further limits online dissent. This development strengthens the case that Pakistan's firewall policies are not only about protecting cybersecurity but also about tightening the wheels over digital spaces in the name of national security. The consideration that a crucial provision has passed without discussion from the public seems to be a most serious concern for its legitimacy and purpose. Given that it happens at a time when states are taking control of online platforms, and social media censorship, the timing of this amendment is significant. Already, Pakistan has been actively blocking websites, restricting VPNs and digital blackouts, and now, with the formation of the Social Media Regulation and Protection Authority, the state will have even greater powers to remove content at will. They limit online freedom and raise worries that Pakistan is moving toward a system of internet control like China's. The new law is so ambiguous that this means any critical voice, journalists, opposition figures, activists; or even ordinary citizens will now be tried in a criminal court for *spreading false information*. It continued in a pattern of the use of cybersecurity laws by the government to stifle political opposition rather than attack misinformation.

This amendment has implications far deeper than legal overreach. It is an attack on Pakistan's digital economy and democratic participation. Public discourse, political mobilization, and economic opportunities, especially for freelancers, startups, and online businesses, have become a space on social media platforms. The blanket bans and higher censorship measures are bad for investors in the tech sector who are pushed into a hostile environment for digital entrepreneurship and global partnerships. Even before the beginning of the current block on X (formerly Twitter) in February 2024, it has already indicated how the state will control the narratives by shutting down those platforms that allow unrestricted discussions. It is worth noting that as these restrictions had already cost Pakistan $1.62 billion in financial terms in 2024, their financial cost will only skyrocket even further, hindering the country's digital future. This amendment exposes a fundamental contradiction: Meanwhile, Pakistan says it is building its cybersecurity infrastructure, but it is simultaneously undermining digital freedoms and economic opportunities. National security laws are based on the logic that they should promote public safety with adequate respect to fundamental rights, yet PECA 2025 puts state prerogative above public empowerment. But it also lacks judicial oversight and independent accountability mechanisms, leaving the government free to regulate, block, and punish online speech arbitrarily defined as *fake information*. In addition to these repressive digital policies, a more recently proposed law the Digital Nation Pakistan Bill ensures these intrusive surveillance technologies with no human rights protections. These developments beg the question: What is Pakistan's digital future, will it be one of security or suppression? And if these trends hold, Pakistan will not be remembered for its cybersecurity progress, but rather for its cyber censorship and human rights abuses. The remedy is not in changing laws to limit freedom, but in changing cybersecurity laws to strike a balance between national security and fundamental rights. The government must immediately withdraw PECA 2025 and begin a sincere dialogue with civil society, digital rights activists, and legal experts before legislating against cyber threats turns into weapons laws against dissent. Firewall technology should be employed to counter the external cyber threat to Pakistan and not be utilized as an internal tool for silencing opposition. Continuing on this path, Pakistan will ultimately cut itself from the global digital economy, isolate its youth, and force independent thinkers into self-censored or exiled. Pakistan faces a serious risk of a controlled and stagnant digital future if action is not taken. Reform is urgently needed.

6. Conclusion

The debate surrounding firewall technology in Pakistan is no longer just about cybersecurity, it has evolved into a critical human rights and governance issue. Firewalls are important for protecting national security, blocking cyberattacks, and safeguarding sensitive data, yet the growing use of such controls as weapons of digital censorship is cause for grave concern. Pakistan's way of setting up firewalls shows a concerning trend of controlling information, where national security is used to limit online freedom. While this article was being written, the amendment to PECA 2025 further solidified these concerns by allowing the state to even more heavily police dissent under the guise of *spreading false information*, in completely ambiguous ways. The growing digital control has economic and political implications. Internet restrictions have already cost Pakistan billions and the financial cost of internet restrictions threatens Pakistan's emerging digital economy, deters foreign investment, and disrupts online businesses. Meanwhile, political censorship through firewalls and social media regulations is undermin-

ing democracy by silencing activists, journalists, and opposition voices. If these trends persist, Pakistan risks being left behind in the global digital sphere, where unrestricted access to information is a major factor in the country's economic and technological development. It is still possible for a balanced approach. If these policies are transparent, legally justified and proportional to the level of security threats, then firewall technology can be used without suppressing free speech. The firewall testing and implementation in Pakistan must be under clear regulations, independent oversight, and judicial accountability. It is also important that cybersecurity laws be reformed through a consultative process with digital rights organizations, legal experts, and civil society to avoid their misuse of political control. Ultimately, it will be Pakistan's choice between security and repression that will determine its future as a digital-free country, an economically progressive country, and a democratic stable one. An open and secure internet is not a contradiction; it is imperative for a modern, progressive Pakistan.

Reference

1. Broderick, J.S., *Firewalls–Are they enough protection for current networks?* Information Security Technical Report, 2005. **10**(4): p. 204-212.
2. Afzal, J., et al., *Review ofVarious Aspects of Digital Violence.* 2024.
3. Ahmadi, S., *Next generation ai-based firewalls: a comparative study.* International Journal of Computer (IJC), 2023. **49**(1): p. 245-262.
4. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024, Springer.
5. Vacca, J.R. and S. Ellis, *Firewalls: jumpstart for network and systems administrators*. 2004: Elsevier.
6. Sharma, H., *Next-Generation Firewall in the Cloud: Advanced Firewall Solutions to the Cloud.* ESP Journal of Engineering & Technology Advancements (ESP-JETA), 2021. **1**(1): p. 98-111.
7. Naseer, I., *Implementation of Hybrid Mesh firewall and its future impacts on Enhancement of cyber security.* 2020.
8. Chatterjee, K., *Design and development of a framework to mitigate dos/ddos attacks using iptables firewall.* International Journal of Computer Science, 2013.
9. Chandel, S., et al. *The golden shield project of china: A decade later—an in-depth study of the great firewall*. in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 2019. IEEE.
10. Aryan, S., H. Aryan, and J.A. Halderman. *Internet censorship in Iran: A first look*. in *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*. 2013.
11. Logan, B.E., *A CASE FOR SOFTWARE-DEFINED NETWORKING IN THE UNITED STATES MARINE CORPS: AUTOMATING DISTRIBUTED FIREWALLS*. 2019, Monterey, CA; Naval Postgraduate School.
12. Gangwar, S. and V. Narang, *A survey on emerging cyber crimes and their impact worldwide*, in *Research Anthology on Combating Cyber-Aggression and Online Negativity*. 2022, IGI Global Scientific Publishing. p. 1583-1595.
13. Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding 'Right to Information'for good governance in Pakistan.* Discover Global Society, 2023. **1**(1): p. 12.
14. Alam, S., *Successful organization change at national database and registration authority (NADRA) Pakistan: a case study.* Global Management Journal for Academic & Corporate Studies, 2013. **3**(1): p. 166-175.
15. Niemi, K., *Engaging security into product development by using baseline security configuration for operating systems.* 2024.
16. Masudi, J.A. and N. Mustafa, *Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age.* Pakistan Journal of International Affairs, 2023. **6**(3).
17. Khan, M.F., A. Raza, and N. Naseer, *Cyber security and challenges faced by Pakistan.* Pakistan Journal of International Affairs, 2021. **4**(4).
18. Saleem, B., et al., *A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap.* International Cybersecurity Law Review, 2024. **5**(4): p. 533-561.
19. Afzal, J., *An Overview of Digital Law*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 1-21.
20. Afzal, J., *Legal Challenges Regarding Digital Operations*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 23-45.
21. Haider, A., S. Raza, and B.Z. Khan, *Organized Crime and the Objectives of the Islamic Penal System.* Al-Qamar, 2023. **6**: p. 63-82.
22. Afzal, J., *Digital Law Enforcement Challenges and Improvement*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 47-78.
23. Castells, M., *The Internet galaxy: Reflections on the Internet, business, and society*. 2002: Oxford University Press.
24. Yongmei, C. and J. Afzal, *Impact of enactment of 'the prevention of electronic crimes act, 2016'as legal support in Pakistan.* Academy of Education and Social Sciences Review, 2023. **3**(2): p. 203-212.
25. Ahmad, A.A.M.D.A., *Deficiencies In peca and proposed amendments to facilitate investigating agencies, courts and prosecution; proper use of electronic devices for effective implementation of law.* International Journal for Electronic Crime Investigation, 2019. **3**(3): p. 6-6.
26. Daudpota, F., *An Examination of Unconstitutional Aspects of Pakistan's Cybercrime Law.* Available at SSRN 2860954, 2016.
27. Haider, A., I. Ahmad, and M. Yaseen, *Jus Cogens and the Right to Self-Determination: A Study of its Peremptory Status and Erga Omnes Effects.* Pakistan JL Analysis & Wisdom, 2024. **3**: p. 59.
28. Afzal, J., *Digital Evidence and Permissibility in Court of Law*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 121-137.
29. Haider, A., *Application of the United Nation Convention against Transnational Organized Crime: An Analysis.* Available at SSRN 4686710, 2024.
30. Afzal, J., *Best Practice of Digital Laws and Digital Justice*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 95-120.
31. Haider, A., A. Ali, and B. Zeb, *Broken Laws, Broken Lives: When Organized Crime Shreds Human Rights.* 2024.
32. Afzal, J., *Future of Legal Tools and Justice*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Editor. 2024, Springer Nature Singapore: Singapore. p. 155-177.
33. Hosein, G. and C.W. Palow, *Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques.* Ohio St. LJ, 2013. **74**: p. 1071.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.10

Review

Identity Theft in the Digital Age: Legal Gaps, Enforcement Challenges and the Need for Global Reform

Sidra Raza[1]* and Shaista Naznin[1]

[1]Department of Law, Abdul Wali Khan University, Mardan, Pakistan

*Corresponding Email: sidraraza82@gmail.com (S. Raza)

Received: 02 December 2024 / Revised: 18 January 2025 / Accepted: 04 February 2025 / Published online: 28 February 2025

ABSTRACT

Identity theft has grown into a major international issue that hurts everyone from individual people to banks and government departments. This research examines international legal frameworks designed to combat identity theft. The study examines critical laws such as the Identity Theft and Assumption Deterrence Act, Theft Penalty Enhancement Act, Fair Credit Reporting Act, and Fair and Accurate Credit Transactions (FACT) Act, among others. The study reveals that inconsistencies in enforcement across jurisdictions reduce the effectiveness of identity theft laws. According to analysis, identity theft keeps growing as one of today's most common crimes because people conduct financial transactions online and cyber security poses significant weaknesses. The results call for better consumer security measures plus stronger connections between federal and state agencies along with new anti-fraud technology. The findings recommend that governments create better data security laws while working together across borders and building better support for victims of identity theft. Ongoing improvement of identity theft laws plus education about it helps victims avoid both monetary loss and emotional distress.

Keywords*:* Identity Theft; Cyber Fraud; International Law; Consumer Protection; Financial Crime, Legal Framework; Data Security; Fraud Prevention; Digital Crime; Cybersecurity Policy

1. Introduction

The main objective of Digital Law is to educate people about the theoretical thoughts relating to the Law and Economics issues in the Digital Environment [1]. Digital identity theft poses serious problems worldwide that affect both individuals and official organizations. The digital revolution has brought unparalleled connectivity and accessibility [2]. Cybercriminals exploit vulnerabilities in digital systems and online transactions to commit identity theft on a large scale [3]. Identity thieves use stolen personal data to rob people of both money and trust, which can lead to legal and financial problems for victims. Identity theft functions through many methods such as stealing credit cards and personal data from databases to create false social security numbers. Identity theft presents more significant problems than just money loss. Thieves can misuse identity information to create false charges, submit fake tax reports, and open medical treatment accounts under false names [4]. Law enforcement finds it difficult to catch up with cybercriminals so governments must create effective anti-crime rules to stop these activities and keep customers safe [5]. The presence of just laws, rules, and regulations that are applied fairly is a sign of good governance [6]. Several different laws operate globally yet challenges like uneven enforcement and legal boundaries make it hard to stop identity theft completely. This research analyzes global identity theft laws, including the Identity Theft and Assumption Deterrence Act, Theft Penalty Enhancement Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act. It evaluates how these laws fight identity theft while showing their weak points in stopping advanced internet fraud. This analysis examines two major aspects of how law enforcement and consumer protection regulations tackle identity crimes. However, there are still gaps in the global legal framework despite the existence of different regulations. With the absence of uniformity of policies between jurisdictions, cybercriminals can exploit the lack of enforcement mechanisms [7]. In addition, there are no strict data security regulations in many regions allowing people and businesses to be breached. The solution to these problems requires internationally coordinated efforts, better legal tools, and improvements in cybersecurity technology.

Objectives of the Study

1. To examine how international laws help to address identity theft and financial fraud.

2. Gaps in the existing legal frameworks are identified to propose strategies for the prevention of global identity theft.
3. To assess the effectiveness of consumer protection laws in shielding people from identification fraud.

2. International Laws on Identity Theft

The majority of states have laws against identity theft that make it illegal to misuse someone else's identifying information [8]. It makes no difference whether the information is financial or personal under the majority of the US state legislation. Social Security numbers, credit histories, and banking PINs are examples of the kind of information that are frequently obtained by:

1. The criminal's unauthorized use of financial and governmental databases to obtain information
2. Identity, credit or debit cards, wallets, and handbags, lost or stolen mail

Identity theft is one of the fastest-growing crimes in the U.S. [9]. Internet usage is common among identity thieves. Nevertheless, they can also get critical personal information from unprotected places like garbage cans, database hacks, and frauds. Identity theft may be prosecuted as a misdemeanor or a felony, depending on your location and the specifics of the offense. For instance, first-time offenders in Illinois may be charged with misdemeanors. According to the Department of Justice, the offense may be considered a felony in several situations under federal law. A person may also face charges of wire fraud, mail fraud, or several other offenses depending on how the offense is carried out. Fraud involving credit cards may also be a part of the offense.

3. The Identity Theft and Assumption Deterrence Act

Congress in 1998 passed the Identity Theft and Assumption Deterrence Act due to high incidences of identity theft and the unenthusiastic reaction from the government towards its victims [10]. Regarding its statute identity theft is now a federal crime. It is a federal offense if an individual ‘‘knowingly and with intent to defraud transfers or uses without lawful authority a means of identification of another person for any unlawful purpose or for obtaining any benefit, advantage or privilege. ” These statutes make it clear that using other people’s identity for unlawful purposes or for obtaining unlawful benefit is a federal offense. One of them under this Act is Identity theft, whereby a person’s information is used to impersonate that particular individual. For a person to be able to perform such an act he/she has to have access to other pieces of information apart from the name of another person. Such other details are the date of birth of a person, social security number, credit card number, and bank account number. It is possible to have several identification documents and identifying numbers, for instance, a driver’s license number. It can involve various forms of Personally Identifiable Information (PII) [11]. The following are the penalties for fraud using identifying document violations: The penalties for using fraudulent identifying document violations depend on the particular offense as well as the type of document that has been violated. For instance, the offender can be fined, or receive a prison term of up to fifteen years if they use the identity of another individual to engage in any unlawful act if they receive anything of value in the aggregate amount of $1000 or more in one year for the commission of the crime. For other offenses, the term in prison is three years. However, if the offense is committed in connection with a violent crime or to facilitate the commission of a drug trafficking felony then the punishment could be up to twenty years. Crimes that are committed with the intent to aid international terrorism are punishable by up to 25 years in jail.

4. The Theft Penalty Enhancement Act of 2004

The Identity Theft Penalty Enhancement Act was passed on July 15, 2004. It amends the identity theft provisions presently in Title 18 of the United States Code and delineates, and prescribes punishment for aggravated identity theft. The law defines aggravated identity theft as a person who ‘knowingly transfers, possess or uses, without lawful authority, a means of identification of another person’ in connection with the commission of specifically listed felonies. In addition to the punishment for the initial felony, aggravated identity theft carries a mandatory two-year prison sentence. In addition to these requirements, the act also provides the US Sentencing Commission with the power to review and amend its guidelines and policy statements to ensure that the guideline offense levels and enhancements adequately punish the identity theft offenses involving abuse of position, and to enforce the laws. The act raised the fines for identity theft at the same time enabled the Justice Department to receive $2,000,000 for the investigation and prosecution of identity theft and related credit card and other fraud cases constituting felony violations of law for FY2005 and $2,000,000 for each of the 4 succeeding fiscal years.

5. Fair Credit Reporting Act

While identity theft is not mentioned in the FCRA, the act can be used to request that the credit reporting agency remove negative information about fraudulent charges or accounts. About the balancing of confidentiality, accuracy, relevancy, and proper use of such information the FCRA seeks to make consumer reporting agencies adhere to reasonable procedures that ensure that needs for consumer credit, personnel, insurance, and other information are met fairly and reasonably to the consumer. Additionally, according to the FCRA, any individual who furnishes information has to ensure that it is accurate and the same applies to consumer reporting agencies regarding the information that they disseminate. According to the Fair Credit Reporting Act (FCRA), consumers have a claim against credit reporting agencies that provide false information about them. An identity theft victim can sue a credit reporting service for negligence in not verifying the information in the consumer report and passing on information that is false due to identity theft. The consumer may sue under the recently amended FCRA at the latest within two years from the time that the plaintiff knew of the violation that led to such liability or within five years from the time the violation occurred [12].

6. Fair and Accurate Credit Transactions (FACT) Act of 2003

Among other things, the FACT Act passed on December 4, 2003, makes several changes to the FCRA to combat identity theft and assist victims [13]. Most of these new regulations that set a national approach to dealing with consumers’ complaints on identity theft and other related frauds are in concordance with legislation enacted by state legislatures. A new FCRA provision also provides for specific steps that credit card issuers, who use consumer credit reports, should follow if they receive a request for an additional or replacement card within a short period after receiving a known change of address for the same account. Other new laws require that social security numbers must be shortened in consumer credit reports if requested by the consumer and credit card account numbers must be truncated in electronically printed receipts to further curb instances of identity theft. Consumers can request fraud alerts on their credit files if they have been victims of identity theft or suspect potential fraud. The new regulations stipulate that a customer may request a fraud alert from one consumer-reporting agency and that agency shall notify the other agencies across the country that the alert has been put in place. Fraud alert records are nor-

mally maintained for ninety days, but the customer can request an extended alert, which is maintained for seven years at most. All the users of the given report are aware of the fraud alert since it is a part of the consumer's credit file. Any created credit score must moreover include the alert. Fraud notice is also given to identity theft victims and at this rate information, related to the crime is deleted from the credit reports of the victims. Upon receiving such proof of the consumer's identity, a copy of the identity theft report, identification of the allegedly fraudulent information, and a statement from the consumer to the effect that the information is not related to any transaction conducted by the consumer, a consumer reporting agency is required to stop all such information from being reported and notify the furnisher of the information in question that it might be the result of identity theft. It is also necessary to provide further consumer reporting agencies to which requests for information blocking can be addressed. The victims of identity theft are also allowed to ask for information concerning the alleged offense. An application and business transaction records of a business entity wherein any transaction which the recipient seeks to assert is a result from identity theft must, upon request of the victim or any law enforcement agency investigating the theft and which is authorized by the victim to receive the records, produce copies of the application and business transaction records to the victim or such law enforcement agency.

7. Fair Credit Billing Act

The Fair Credit Billing Act (FCBA) grants customers an opportunity to have charges that were made by an impostor removed from their accounts and also an opportunity to receive an explanation of the charges that have been made and confirmation of such charges [14]. However, it is not a statute that was put in place to deal with identity theft in particular. The FCBA was adopted to safeguard the consumer against misleading and unjust credit billing and credit card practices Consumers are explained and protected by law against unfair billing problems within consumer credit transactions. According to the FCBA, billing error refers to an unauthorized charge, a charge for goods or services for which the consumer has requested an explanation or confirmation in writing, or charges for products and services that were never furnished or received by the consumer. To have billing irregularities rectified, a customer can claim the FCBA from the creditor. Thus, the customer is not bound to pay the protested amount, the creditor is prohibited to attempt to collect any part of the protested amount together with the interest, and other expenses incurred in connection with the extension of credit. The act also prescribes how such matters should be addressed and it provides that the consumer's claims should be considered. If the creditor finds the existence of the stated billing error, he or she will be in a position to correct the mistake and credit the consumer's account with the amount in dispute inclusive of finance charges.

8. Electronic Fund Transfer Act

The Electronic Fund Transfer Act, like the Fair Credit Billing Act, though does not mention identity theft, does provide customers with a legal way to challenge transactions that they did not authorize and to have their accounts replenished in the case of error. The Electronic Fund Transfer Act (EFTA) aims to give the fundamental architecture that sets the rights, duties, and risks of users in EFT systems [15]. The EFTA also limits consumer's responsibility for any unauthorized electronic fund transfers, for example. The consumer's responsibility is capped at $50 or the amount of the unauthorized transfers before the institution receives the consumer's notice of the loss or theft of a debit card or other device used in making electronic transfers, which must be given within two business days of discovery. The financial institutions must also provide a customer with a confirmation of any electronic fund transfer, which the customer initiated from an electronic terminal. A financial institution must examine a potential mistake, find out whether or not it has happened, and notify the consumer of the findings and determination in writing or by mail within ten business days if it is provided with an oral or written communication from the consumer to the effect that the documentation forwarded to the consumer contains an error within sixty days from the date of forwarding such documentation. The consumer's name and account number must be included in the notice to the financial institution, together with the following information: the consumer's perception of an error, the actual amount of the error, and the justification for perceiving the error in the paperwork. Financial institutions are required to investigate errors and resolve disputes promptly under relevant regulations. If the financial institution cannot finalize the investigation within ten business days, they may recredit the customer's account for the amount in question as a temporary measure. This will help in the conclusion of the investigation and dismissal of the chance of an error being made.

9. Identity Theft Task Force

In April 2007, the President's Identity Theft Task Force released its final report with a plan to combat identity theft. The plan focuses on using government resources, protecting personal data, assisting law enforcement, educating businesses and consumers, and improving security measures in both public and private organizations [16]. The Plan focuses on four main areas of improvement: protection of consumer's identity from identity thieves due to improved security and awareness; making it difficult for the thief to get consumer's data, helping the victims of identity theft to recover, and deterring identity theft through more active pursuit and punishment. To ensure that more offenses of identity theft can be prosecuted at the federal level, the Task Force provided the following recommendations that targeted filling up perceived gaps in federal criminal laws. They are listed below:

1. Expand the list of predicate offenses for aggravated identity theft offenses
2. Reform the statute that enshrines electronic data theft law by doing away with the provisions that state that the information should have been stolen through interstate communication [17].
3. Sanction the makers and disseminators of the nasty spyware and keyloggers.
4. Extend the cyber-extortion statute to capture other forms of cyber-extortion.
5. Provide for the possibility of an enhanced sentence for identity thieves who defraud data belonging to companies and organizations.

10. Real ID Act of 2005

The DHS made the final rule on January 11, 2008, about the REAL ID Act of 2005 on State-issued driver's licenses and ID cards that federal agencies would be allowed to accept for official use starting May 11, 2008. The Real ID Rule lays down mechanisms for meeting the REAL ID Act's basic standards. These standards are regarding the various aspects that surround the overall procedure of issuing an identity document; the information and the security aspects that should be incorporated into each card; the identity, U. S. citizenship or legal resident status of the applicant; the validation of the source documents which the applicant presents; and the security features about offices wherein the cards are issued. Any state that has presented its petition before the last date of the year December 31, 2009, will have its extensions granted. In

addition, the second renewal is also possible up to May 10, 2011, if some conditions concerning the security of the license and identity procedures, as well as the credentials of the states, are met. For persons born after December 1, 1964, the Rule brings the enrollment period to December 1, 2014, and for those born on or before December 1, 1964, the enrollment period is on December 1, 2017, to replace all licenses that are to be used for official purpose by the states that have been deemed to comply with the act by the DHS to have all their cards to The policy took effect beginning of the fiscal year on the 31st of March 2008 (Stevens, Federal laws related to identity theft, 2008).

11. Key Findings

International identity theft laws are analyzed to show significant gaps in legal enforcement, cross-border cooperation, and consumer protection. Incentives and enforcement are needed when regulations are not enough [18]. The most important finding is the inconsistency of identity theft laws in different jurisdictions. In the United States, the Identity Theft and Assumption Deterrence Act and the Theft Penalty Enhancement Act impose strict penalties for offenders, but many countries have no such legal frameworks that would enable cybercriminals to take advantage of the lack of regulatory environment. This disparity gives rise to a shelter for international criminals operating in several countries who are difficult to track and prosecute by law enforcement agencies. A major issue with identity theft legislation is its reactive nature. Most legal frameworks are geared towards punishment rather than preventing identity theft in the first place. Fair Credit Reporting Act (FCRA), and Fair and Accurate Credit Transactions Act (FACTA) only afford some consumer protections, but they are only useful to victims after the fraud has occurred. Data security laws are still largely absent of proactive measures, leaving individuals and businesses vulnerable to continued risk in the face of ever-changing cybercriminal tactics. Stronger data protection measures are necessary including stronger encryption, biometric verification, real-time fraud detection systems, and so on. Furthermore, identity theft laws are still only enforced with difficulty. Extradition and prosecution are difficult in jurisdictions where legal action is minimal or nonexistent, allowing many offenders to operate. An increasing trend in trade and investment is determined by several factors [19]. Financial institutions tend to prioritize business efficiency in preference to robust security, which results in weak authentication processes that do not detect fraudulent activities. The increase in identity theft cases has greatly contributed to the failure of institutions to adopt stringent cybersecurity protocols.

12. Conclusion

Identity theft is a global economic and security threat, not an individual crime, and it demands urgent coordinated legal intervention. While the existing legal frameworks deal with some aspects of identity theft, they are not comprehensive and proactively oriented. Without strong global cooperation, identity thieves will continue to exploit legal loopholes, leading to financial and psychological distress for victims. To address this problem, governments should stop using punitive measures and focus instead on preventive measures, like data encryption, stricter authentication protocols, and international cooperation in tracking cyber criminals. Consumer data security must be a priority for financial institutions to secure consumer data and implement stronger verification measures, along with speedy responses to fraud reports. Identity theft must move from reaction to prevention, with a strong focus on data security, consumer protection, and international legal cooperation. Identity theft can only be curtailed and its devastating consequences can only be diminished through comprehensive legal reform and technological improvements.

Declaration

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement: This article is extracted from chapter 3 of the thesis of Miss Sidra Raza (Crime of Identity Theft in Pakistani Law: A Critical Analysis, under the supervision of Dr. Shaista Naznin from Abdul Wali Khan University, Mardan, Pakistan.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] C. Yongmei and J. Afzal, "Impact of enactment of 'the Prevention of electronic crimes act, 2016 ' as legal support in Pakistan," *Acad. Educ. Soc. Sci. Rev.*, vol. 3, no. 2, pp. 203–212, 2023.

[2] A. Haider, A. Ali, and M. Zubair, "Chasing Dragons in the Dragon's Land: A Convoluted Struggle with Drugs and Deviance in Modern China," *Asketik J. Agama dan Perubahan Sos.*, vol. 7, no. 2, pp. 322–343, 2023.

[3] A. Haider, U. Yousaf, N. H. Shah, and W. Azeem, "UNTOC's Role in Combating Transnational Organized Crime: An International Response," *Pakistan J. Law, Anal. Wisdom*, vol. 3, no. 8, pp. 178–188, 2024.

[4] J. Afzal, C. Yongmei, A. Fatima, and A. Noor, "Review of various Aspects of Digital Violence," 2024.

[5] A. Haider, "Application of the United Nation Convention against Transnational Organized Crime: An Analysis," *Available SSRN 4686710*, 2024.

[6] J. Afzal and C. Yongmei, "Federal and provincial legislation regarding 'Right to Information for good governance in Pakistan," *Discov. Glob. Soc.*, vol. 1, no. 1, p. 12, 2023.

[7] A. Haider, S. Raza, and B. Z. Khan, "Organized Crime and the Objectives of the Islamic Penal System," *Al-Qamar*, pp. 63–82, 2023.

[8] G. R. Newman and M. M. McNally, "Identity theft literature review," 2005.

[9] S. B. Hoar, "Identity theft: The crime of the new millennium," *Or. L. Rev.*, vol. 80, p. 1423, 2001.

[10] M. A. Sabol, "Identity Theft and Assumption Deterrence Act of 1998-Do Individual Victims Finally Get Their Day in Court," *Loy. Consum. L. Rev.*, vol. 11, p. 165, 1998.

[11] P. M. Schwartz and D. J. Solove, "The PII Problem: Privacy and a new concept of personally identifiable information," *NYUL rev.*, vol. 86, p. 1814, 2011.

[12] F. C. R. Act, "Fair Credit Reporting Act," *Flood Disaster Prot. Act Financ. Inst.*, 2009.

[13] M. Epshteyn, "The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers," *Geo. LJ*, vol. 93, p. 1143, 2004.

[14] A. J. Walden, "Closing the" No Further Responsibility" Loophole in Resolving Credit Billing Errors," *Wayne L. Rev.*, vol. 66, p. 321, 2020.

[15] L. M. Taffer, "The Making of the Electronic Fund Transfer Act: A Look at Consumer Liability and Error Resolution," *USFL Rev.*, vol. 13, p. 231, 1978.

[16] K. M. Finklea, *Identity theft: Trends and issues*. DIANE Publishing, 2010.

[17] A. Haider, "Beyond Borders and Bars: Exploring the Transformative Influence of the UN Convention against Transnational Organized Crime," *pjlaw.com.pk*, vol. 2, 2023, doi: 10.1080/09766634.2011.11885550.

[18] I. Ahmad, A. Haider, and B. Zeb, "In the Name of Nature: The Legal Frontiers of Environmental Preservation," *J. Asian Dev. Stud.*, vol. 12, no. 4, pp. 401–411, 2023.

[19] I. Ahmad, A. Haider, and J. Afzal, "The Geopolitical and Economic Impact of BRICS on the Middle East," *FWU J. Soc. Sci.*, vol. 18, no. 4, pp. 80–95, 2024.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.9

Perspective

Artificial Intelligence in Autonomous Weapon Systems: Legal Accountability and Ethical Challenges

Ibrar Ahmad[1*], Laila Ahmad[2], Naila Irshad[3] and Muhammad Talha[4]

[1]School of International Law, Southwest University of Political Science and Law, China

[2]School of Economics, Southwest University of Political Science and Law, China

[3]University of Gujrat, Pakistan

[4]Government Post Graduate College Mardan, Pakistan

* Corresponding Email: ibrarahmad557@gmail.com (I. Ahmad)

Received: 23 October 2024 / Revised: 26 December 2024 / Accepted: 19 February 2025 / Published online: - 28 February 2025

ABSTRACT

Autonomous Weapon Systems (AWS) are reshaping modern warfare, offering enhanced operational efficiency but raising significant legal, ethical, and regulatory concerns. Their capacity to engage targets without human intervention creates an accountability gap, challenging the application of International Humanitarian Law (IHL). The current legal frameworks are incompetent to define meaningful human control. That complicates the attribution of responsibility when AWS violate human rights. Ethical challenges, including the dehumanization of warfare, algorithmic biases, and indiscriminate targeting, jeopardize civilian protection. Moreover, the proliferation of AWS amplifies global security risks, particularly with their potential misuse by non-state actors. This paper critically examines these challenges, evaluating current legal frameworks, ethical considerations, and regulatory inconsistencies. It proposes war torts, corporate accountability, transparency measures, and binding international treaties to address governance gaps. Supports international cooperation and oversight mechanisms is essential to ensure AWS comply with IHL and human rights law. This research contributes to the global discourse on autonomous warfare, offering practical policy recommendations for ethical and legal governance.

Keywords*:* Artificial Intelligence; Autonomous Weapons System; International Law; Proliferation

1. Introduction

The fast development of autonomous weapon systems (AWS) transforms traditional war practices. AWS operates independently because these systems recognize and strike targets without requiring human intervention [1]. The autonomous capability brings important benefits including high accuracy, reduced personnel danger and better resource management [2]. The advantages of these systems come at the expense of critical disadvantages. AWS create multiple complicated issues because they execute deadly actions without human supervision. In 2020, a drone strike in Libya marked the first reported use of an AWS in combat, igniting global debates about accountability, compliance with international humanitarian law (IHL), and the moral implications of delegating life-and-death decisions to machines [3]. The growing adoption of AWS technologies threatens to reduce legal compliance while reducing human dignity and destabilizing principles [4]. The challenges require both enhanced regulatory frameworks and fundamental reforms of accountability frameworks for warfare systems controlled by artificial intelligence.

The accountability gap represents a legal and ethical conundrum because AWS violations of both IHL and human rights remain without responsible parties [5]. Autonomous systems present a problem when traditional legal concepts of mens rea (intent) and actus reus (action) are designed for human decision-makers. The absence of consensus about "meaningful human control" stands as an obstacle to AWS regulation because the concept lacks a clear definition [6],[7]. A programming failure that leads an AWS to strike a civilian building produces three possible defendants: the developer the military commander or the government. Without well-defined liability protocols, victims cannot pursue legal recourse that subsequently degrades trust in existing laws. The traditional military hierarchy faces disruption through AWS while states find it challenging to assign responsibility because of these systems'

unique operational characteristics [8]. IHL alongside other legal frameworks fail to provide sufficient solutions for addressing the distinctive challenges created by AWS. According to Boothby the application of distinction and proportionality principles proves challenging for autonomous weapons systems that function independently [9]. AWS systems experience difficulties distinguishing between armed combatants and ordinary innocent civilians which can result in IHL violations [10]. Machines cannot perform human-level assessments of moral and strategic factors [11],[12]. That constitutes proportionality because this judgment process depends on human decision-making abilities[13]. The rising concept of "meaningful human control" shows potential in solving legal concerns but its unclear definition and irregular applications have delayed progress [14]. The absence of clear guidelines creates two major problems: reduced accountability and unexpected governance gaps which prevent the world from properly responding to AWS threats.

The ethical challenges of AWS create supplementary difficulties. Machine-based selection of lethal choices in warfare threatens to dehumanize combat operations. The absence of empathy and moral judgment together with an inability to grasp complex human life characteristics makes machines unable to make ethical warfare choices [15],[16]. Technological advancement results in organised forces more easily and causes more destruction and suffering [17]. The susceptibility of AI algorithms to biases represents an additional threat because they might enable processor targets along with causing unacceptable damage to particular populations [18],[19]. AWS systems remove moral accountability from life-and-death decisions according to deontological ethics [20]. The AWS achieves harm reduction outcomes by maintaining soldier survivability [21]. The potential benefits from AWS systems remain untapped because of unresolved ethical and legal issues they generate. Achieving a balance between technological development and moral standards exists as both a practical requirement and a formal moral duty. At the international level regular progress towards AWS regulation remains challenging because of global political disharmony coupled with national interests. Under the United Nations Convention against Certain Conventional Weapons (CCW) countries try to find solutions but agreement remains doubtful [22]. Most nations support the principle of human control over AWS. However, they cannot agree on what meaningful human control requires nor how to implement it [23]. China demonstrates this contradiction between global commitments to AWS bans and its ongoing substantial investment in military AI systems [24]. The disagreements about AWS frameworks highlight the pressing demand for binding international rules that protect human rights [25].

The analysis of this study focuses on these problems through an investigation of AWS accountability gaps together with existing legal framework inadequacies and ethical concerns. The paper evaluates three solution approaches by analysing war torts alongside transparency measures and corporate accountability while examining their respective strengths and limitations. The research examines global initiatives to control AWS under international law. In response to AWS challenges, this paper proposes a framework that maps legal rules to ethical values and regulations. This guide shows that technological advancement must be complemented with institutional responsibility and human dignity while presenting ways to maintain proper autonomous technology usage. The research findings can therefore be used for future governmental action on how to regulate this rapidly emerging area.

Key Research Questions:

How do autonomous weapon systems (AWS) create legal and ethical problems regarding IHL compliance and accountability issues?

What changes should be made to current legal structures to control AWS technology while holding those who break rules accountable?

The research addresses an expanding body of AWS studies through a proposed framework that integrates legal analysis with ethical matters and regulatory considerations. This work presents actionable solutions through war torts and corporate accountability. To bridge liability gaps while maintaining compliance with International Humanitarian Law. The research findings will help shape current discussions and future regulatory efforts within this fast-developing domain.

2. Literature review

The deployment of AWS has created legal, and ethical dilemmas and regulatory questions like no other conventional technology. Exclusively operated weapon systems present new challenges to traditional approaches to liability and International Humanitarian Law implementation.

2.1. Accountability Gaps in AWS and IHL Compliance

Multiple studies indicate significant deficiencies exist while dealing with the accountability gap; such as ethical challenges and regulatory discrepancies. The research reviews current studies to determine knowledge gaps before showing how this paper addresses those deficiencies. According to Crootof, AWS disrupts the current legal frameworks because these systems eliminate humans from making key decisions [26]. When IHL and human rights violations occur without proper accountability systems, then it becomes difficult to prosecute because victims cannot access legal remedies [27]. The automatic nature of AWS systems generates ambiguous boundaries of responsibility just like who bears legal accountability developers, commanders, or the states [28]. Verdiesen et al., demonstrate that meaningful human control demands technical monitoring combined with active human oversight to guarantee compliance with IHL [29]. The current literature failed to explore this conception, which indicates a significant deficiency in existing knowledge. This research examines the accountability gap through critical analysis followed by proposals for war torts and improved oversight systems. This research examines which mechanisms help to identify responsible parties while guaranteeing legal redress for violations committed by AWS.

2.2. Ethical Concerns: Lethal Decision-Making by Machines

The concern about the moral dimensions arises from having machines handle important death-dealing decisions. Some critics maintain that when AWS assumes lethal decision power, it removes the human effort in making judgements to determine life and death matters. According to Sparrow, machines do not possess empathy and the ability to reason ethically as mandatory elements for decision-making [30]. The way autonomous weapons operate creates doubts about both discriminatory targeting methods and unintended harm that primarily affects vulnerable groups [31],[32].

2.3. Algorithmic Biases and Their Ethical Implications

The built-in biases within AI algorithms function to intensify the above-mentioned ethical challenges. Studies show that algorithmic biases produce discriminatory results that violate fundamental principles of fairness and justice in military conflicts [33]. AWS may reduce the total amount of harm to soldiers through protective measures, but their ethical problems need resolution before this potential benefit can materialise [34]. Current research shows that establishing complete ethical frameworks requires human control together with rational moral processes and IHL compliance.

This research develops previous arguments by demonstrating that ethical guidelines must be implanted throughout AWS design stages and operational phases. This research covers the identified ethical gaps that appear throughout existing literature. The global regulations of AWS face numerous considerable obstacles.

2.4. Regulatory Challenges and Global Governance of AWS

The United Nations Convention on Certain Conventional Weapons (CCW) stands at the centre of international discussions about regulating autonomous weapon systems. According to Docherty, the international community struggles to reach an agreement on fundamental issues, including the definition of meaningful human control [35]. National security priorities, along with technological progress, result in opposing viewpoints between states that prefer human control of AWS systems. Due to these regulatory inconsistencies, there are gaps in global governance, the main obstruction to enforcing International Humanitarian Law standards [36]. The research addresses framework limitations by implementing international agreements together with mandatory operational guidelines. The research facilitates AWS regulatory development through standardized definitions and global collaboration platforms.

2.5. Security Risks and Misuse of AWS Technology

The AWS platform serves two functions which allow unauthorized groups including non-state actors and rogue states and criminal organizations to exploit these capabilities. Such risks intensify because no effective international system exists to monitor these developmental processes. The spread of AWS technology creates unstable situations in regions and intensifies existing humanitarian emergencies as Verdiesen et al., argue. The literature demonstrates the necessity of creating powerful universal agreements to regulate AWS use. Boothby explains how export control systems together with monitoring systems provide essential authorization control for these technologies [9]. International collaboration faces significant obstacles because states fail to work together. The research outcomes will help to define improved international standards for arms control as well as intergovernmental cooperation aimed at counteracting the misuse of AWS technologies. The research successfully balances the technological advancement and the security measures of the global world together with the humanitarian needs. Studies indicate that the regulatory structure of AWS is composed of several critical flaws. Business activities within AWS encounter challenges because of the absence of clear procedures since the current human rights and humanitarian protection frameworks do not have effective ways of sharing responsibility. Inadequate accountability systems that remove legal redress from the victims effectively lead to a fatal blow to the doctrines of the rule of law. Modern frameworks are lacking in creating enough ethical standards that address the ethical issues of the use of AWS technology in automated death decisions. International progress for effective frameworks remains low due to poor standard operational procedures of the regulatory institutions and the failure to develop standard definitions of human control. AWS technologies have relatively few restrictions that put into place risks that make non-state actors and rogue states use these technologies. It is a qualitative work, which focuses on ethical issues and legal analyses to provide solutions for the identified gaps. The combination of the legal parameters and ethical principles along with the regulatory safeguard provides an effective framework that ensures the protection of human value along with the humanitarian law standard for AWS.

3. Methodology

The study adopts the quantitative research method to examine the challenges that result from the use of autonomous weapon systems (AWS). The study focuses on the primary legal sources, the Geneva Conventions, the UN Convention on Certain Conventional Weapons (CCW) and International Committee of the Red Cross reports. The research gathers its information through the analysis of journal articles and case laws. The research explores the approaches in which autonomous systems are granted lethal decision-making power through an ethical perspective that is a blend of deontology and utilitarianism.

4. Analysis

The rapid development of Autonomous Weapon Systems (AWS) leads to various legal questions ethical challenges and regulatory framework difficulties. This scenario of operation autonomous systems raises fundamental questions regarding IHL compliance and accountability frameworks. Technological progress in this area creates complex circumstances involving legal liability, ethical matters and global security risks.

4.1. Accountability and Legal Responsibility

The literature shows substantial concern about AWS operations due to insufficient responsibility tracking systems. The ICRC (2016) clarifies that due to unclear accountability guidelines, the violations of IHL or human rights standards face difficulties [37]. AWS operations frequently lack meaningful human control which makes it difficult to determine legal accountability for violations. A lack of personal responsibility raises critical difficulties for those seeking justice [38]. Traditional legal concepts which include mens rea and actus reus fail to work properly when used to analyze autonomous systems operation. The accountability deficit is an important issue as it comes from the lack of assigning human agency in the case of AWS. Even in human-controlled military systems, responsibility can be attributed; however, AWS complicate this issue by operating autonomously. The consequent confusion of who is to blame, most especially when the actions of AWS are damaging or against the law, erodes the efficiency of legal systems. Interestingly, human intervention is important in addressing these challenges since it guarantees that decision-making can always be traced to humans. According to McDougall, the number of human actors involved in each system is the best way to assign responsibility when there are AWS violations [39]. Verdiesen et al. claimed a high level of proactive human oversight measures that would guarantee accountability. While McDougall concentrates on the role of human control in situations that require accountability. Verdiesen suggests enhancing the framework of technical and potentially reportable and manageable mechanisms, including human supervision. There is a gap in the current legal frameworks; there is no precise definition of meaningful human control. Such a situation creates confusion that arises and hinders any attempts by the states and international organisations for improved accountability. The lack of a standard for AWS responsibility poses no action against the perpetrators and undermines IHL compliance.

4.2. Ethical Implications

It is hard to describe the ethical potential of AWS, although the issue of lethal choices is rather crucial here. McDougall claims that to become effective killers, AWS does not need practical moral reasoning when it comes to choosing between life and death[40]; which could entail disproportionate lethal force and additional suffering. In the same manner, Verdiesen et al., note that AWS might dehumanise warfare by bringing the lethal force to a higher level while decreasing the moral aspects of warfare and raising the probabilities of discriminative targeting. The autonomous weapons sys-

tem (AWS) faces a serious ethical issue because it lets machines autonomously determine when to kill the targets. Due to their programming, AWS lack the built-in ability that human soldiers possess to analyse moral effects before making decisions. AWS systems cannot make judgements about human life, which demonstrates their inadequate ability to perform critical decisions. Discriminatory targeting poses a serious ethical problem because AWS algorithms could display bias that causes human rights violations resulting in excessive harm to civilian populations. The authors agree ethical frameworks are essential; however, they implement different strategies to enforce humanitarian principles with AWS. McDougall proposes new ethical guidelines for military use, while Verdiesen et al. emphasize that frameworks must be created to direct AWS operations. This shows an important lack of ethical oversight for AWS, which especially affects its ability to make moral decisions automatically. The absence of ethical guidance creates a situation that can harm humans by violating both human dignity standards and human rights. An urgent need exists to establish ethical regulations that will protect humanitarian law while upholding human values during AWS deployment.

4.3. Regulation of Autonomous Weapon Systems

The current legal systems fail to control AWS because these systems operate independently. Due to its imprecise definition of human oversight, the UN Convention on Certain Conventional Weapons (CCW) covers some issues but achieves no agreement (ICRC, 2016). States advocate for different approaches regarding military technology autonomy because some states want strict regulations, but others prioritize operational effectiveness. The conflict between human oversight and autonomy represents a worldwide dispute about the proper position of technology within military operations. Advanced technological states stand against strict regulation because they believe enhanced autonomous warfare capabilities lead to better military performance. States focused on human rights and International Humanitarian Law require human involvement for both legal compliance purposes and to prevent violations. According to Verdiesen et al., the regulation of AWS requires robust human oversight because clear guidelines serve to protect against IHL violations. The ICRC supports international cooperation to develop common standards for AWS yet McDougall indicates that technical limitations must be resolved to maintain compliance with IHL. The inability to agree upon specific human intervention standards continues to block effective AWS regulation methods. Modern autonomous technology moves too quickly which renders existing legal frameworks outdated; while preventing them from guaranteeing both International Humanitarian Law compliance and human rights protection in autonomous warfare.

4.4. The Threats and Global Security

The increasing adoption of AWS technologies generates substantial threats to worldwide security. According to Sending Up a Flare (2020), AWS demonstrates dual-use capabilities that non-state actors rogue states and criminal organizations could acquire [41]. The uncontrolled expansion of AWS technologies creates conditions which amplify humanitarian disasters and diminish world peace stability. The rapid expansion of AWS systems creates an important security concern for international stability. Systems controlled by non-state actors may be utilized in ways that break IHL and human rights law. Conflicts will experience increased humanitarian suffering when AWS technology gets deployed to regions without established protections under International Humanitarian Law. Research shows how widespread AWS system deployments create safety risks. The authors at Verdiesen et al., advocate for international governance structures to manage AWS distribution yet Sending Up a Flare (2020) argues global institutions need to track non-state actors to prevent misuse. The world currently operates without defined regulatory frameworks that would manage the international distribution of AWS technology. International supervision of non-state actors remains absent which allows these technologies to flow freely while creating unpredicted future uses and volatile diplomatic relationships.

5. Discussion

The study explores the accountability frameworks and IHL regulatory structures to examine the challenges of Autonomous Weapon Systems. The constant pace of development of AWS systems results in unpredictable situations. Such as limitless ethical responsibilities the lack of adequate legislation and regulation, and insufficient mechanisms of control. AWS technologies contribute to the development of more perilous international security conditions with their expansion of international operations. This study indicates the necessity of elaborating precise legal norms as well as comprehensive ethical standards and international collaboration frameworks to address these emerging issues.

5.1. Ethical and Accountability Challenges of AWS

The AWS technologies contribute to the distressing international security situations with their increase in international operations. This study outlines the need to formulate concrete legal frameworks, comprehensive ethical standards, and international collaboration protocols to meet these emerging concerns. The analysis reveals that the chasing of accountability gaps is the most important issue interpreted by the research on AWS. An autonomous execution of AWS with no human oversight creates an almost impossible task of attribution for any probable human rights or International Humanitarian Law violations. As an example “In the case of the 'Sentry' project by the US military, accountability became problematic with AWS obtaining autonomy in decision-making that led to civilian casualties, but human commanders were absent from overseeing the actions of the machines.” The analysis reveals that tracking responsibility gaps are the most significant critical issue that research uncovers in AWS. Lack of human control over AWS means that finding those responsible for human rights or International Humanitarian Law violations becomes nearly impossible when systems are fully autonomous. Human supervision failures are the primary barriers to identifying the responsible entities during autonomous system misuse or harming events. The vagueness of the definitions of meaningful human control leads to legal ambiguity which denies victims adequate justice while at the same time degrading the IHL compliance system performance.

5.2. Human Control and IHL Compliance

The issues of ethical concern in AWS require similar treatment. Lethal decision-making computer systems pose a risk whenever there is no human moral input involved in the process. Because the lack of moral input leads to prejudice targeting and war desensitization. AWS systems are not capable of assessing human costs from decisions that generate enormous violence and additional suffering as stated by McDougall in 2023. Military conflict zones would grow significantly because IHL compliance does not exist or is limited in these areas and biased algorithms meet human rights violations. While the UN Convention on Certain Conventional Weapons (CCW) attempts to govern AWS, it does not even establish baseline norms for human-machine interactions after adhering to the norms of International Humanitarian Law. The fast-changing nature of technology also slows down the formulation of standard laws because states have no conventions regarding AWS control. For instance, the failure to explain what constitutes 'meaningful human control' in the CCW framework led to instances. In the

course of the conflict in Libya, a fully robotic AWS targeted civilian infrastructure without definitive human control." This example gives a real-world context to how a lack of clearly defined human control translates into operational failures.

5.3. International Humanitarian Law and Regulatory Gaps

The AWS technologies have continued to grow, and the current surge is a significant threat to international security. The increased availability of AWS technology systems creates a great number of security threats that enable non-state actors, and rogue states, criminal organizations to exploit these systems. The lack of international regulations in the framework of global governance would allow for numerous serious violations of IHL and create regional insecurity, and humanitarian crises. This research follows McDougall's and Verdiesen et al.'s position that AWS systems should not have moral reasoning abilities. Two of the ethical issues noted by both research studies are the dehumanization of warfare targets. This means that McDougall military ethics required fundamental changes still Verdiesen emphasizes the creation of such standards that would support AWS's compliance with humanitarian objectives. The study supports Verdiesen et al.'s and the (ICRC's 2016) view on having standard international regulation and collective effort. In 2021, the UN debated the incorporation of AWS into international law but failed to propose a definition of "meaningful human control. Thus, it has further delayed the implementation of a binding treaty. AWS hence becomes one more arena for further regulatory delay, now owing to the lack of an international consensus in favor of its existence.

The study revealed that there are differences in understanding the concept of meaningful human control definitions along with challenges toward international coordination in regulation. These are findings that show that the world requires good legal frameworks to deal with existing issues as evidenced by research findings. The findings of prior studies reveal that modern legal instruments do not allow for addressing the complex challenges that AWS systems entail. The accountability measures are still weak, and there are no agreed human control definitions, which is why AWS system governance remains unsuccessful. The human rights implications of machine-initiated and/or machine-executed lethal operations should be discussed by ethicists right away. The increasing integration of AWS technology systems presents new challenges to global security systems during their deployment around the world. AWS systems that are operational and provide access to non-state actors create multiple security threats that threaten worldwide peace systems.

6. Recommendations

6.1. Closing the Accountability Gap

There are clear expectations under interstate law that provide for human oversight across all AWS systems under AWS. Every functional aspect of the AWS systems requires a human-controlled interface protocol for monitoring the operator's activity. Two new war torts should be created as legislative instruments to define state liability in the event when autonomous warfare systems need to be adjusted beyond recognition. The elements of victim remedies when combined with enhanced accountability tools form a good solution.

6.2. Developing Ethical Guidelines

AWS lethal decision systems require full ethical frameworks as the foundation of their working processes when integrating moral reasoning at the stage of real-life implementation. Active human oversight should protect the operational architecture of AWS platforms because such processes should not be discriminative or dehumanizing when war is waged. To achieve ethical consistency in the world, the world requires international organizations to devise ethical principles with international jurisdiction.

6.3. Strengthening Regulatory Frameworks

The current international legal systems do not have enough power to regulate the AWS systems operations. It is necessary to include standard operational conditions and compliance with the International Humanitarian Law standards in an international treaty to regulate AWS systems that need human control. International humanitarian law requirements only allow organizations to create AWS system operational procedures where AWS systems are defined as specifically as possible. Such operational standards with international support reflect the most critical priorities that the world community should focus on.

6.4. Mitigating Proliferation Risks

There is a need to have enhanced international architecture to control the security risks that accompany dual-use technology advanced through AWS systems. There is a need for implementation of the global monitoring protocols and export control systems to fight against breaches from rogue state actors and unauthorized non-state actors. The world needs collective action toward the cessation of wars employing AWS technology without undermining security systems in volatile areas. The systemic development of AWS technology challenges institutional control and ethical behavior benchmarks. There are important ethical challenges for autonomous systems that need solutions now and improvements in currently lacking legal frameworks. To preserve and protect human rights the members of the international community should establish general rules regarding AWS deployment that are aligned with the parameters of IHL. These technologies require higher levels of protection protocols and far improved weapons control mechanisms because of their global deployment capabilities. For the international community to get the maximum contributions to global security and peace there is the need to embrace general regulatory standards and ethical rules that eliminate the risks associated with AWS.

7. Conclusion

The scientific study was devoted to the identification of the main legal constraints ethical issues and regulatory challenges that are inherent in Autonomous Weapon Systems (AWS). It remains today's modern warfare system but it is still lacking adequate legal structures to meet new operation needs. Again during this analysis, there is a clear legal vacuum because definitions of AWS system responsibility for human rights abuse and International Humanitarian Law violations are still lacking. The criticism presented significant ethical issues with automated lethal decision systems, which entirely lack compassion and possess low average moral reasoning and human outcomes prediction capacities. The first and foremost risk of fully autonomous operations lies in the fact that it is unclear which organization has to take on the blame for actions initiated by the system. The current insufficient human-operated system capacities to adequately control autonomous processes give rise to AWS governance to proactively shape more legal solutions. The implementation of the globally agreed regulatory frameworks poses significant challenges for the adoption of opposed national positions on human system control. The absence of AWS operational standards leads to ethical issues of discrimination since algorithmic decisions create targets and dehumanise warfare capacities as well as exacerbate human rights abuses through biased actions. The AWS technologies are felt to pose significant threats to global security frameworks due to proliferation risks because of the following:

These technologies have two purposes at once, which pose enormous threats of misuse whenever they are employed by individual actors and non-adherent countries. AWS systems escalate and proliferate because there is no law to govern them and this deviously contributes to undermining regional security by generating more unlawful warfare scenarios that compromise IHL's role in preventing civilian victimization.

This research investigates current AWS regulation methods with emphasis on the UN Convention on Certain Conventional Weapons (CCW) framework. These regulatory frameworks have some implementation issues owing to vague definitions and variable global applications that create unregulated oversight domains. Scholars and academics alike persist in their discussion of the best approach to AWS technology deployment through methods that either rely on human intervention for regulation or methods that entail ethical requirements that require human intervention for risk minimization. Multiple proposed solutions attempt to address the recognized issues. The development of precise human management guidelines for AWS operations by literature should precede international governments' regulatory standards. The development of war torts needs to occur to preserve state liability when human actors are not directly involved. Total ethical frameworks must be developed to allow AWS compliance with human rights obligations and protection of human dignity. Moral reasoning and human monitoring standards must become essential elements for the entire AWS development process beginning with design and extending to deployment stages. AWS technology proliferation needs worldwide agreements and global monitoring organizations to protect systems from unauthorized activities by non-state actors. AWS technologies demonstrate great military potential but need comprehensive ethical rules and regulatory adjustments to sustain their fast development through international collaboration. International standards need development to achieve responsible AWS deployment that upholds International Humanitarian Law standards and safeguards human rights with human dignity. The safe integration of artificial warfare systems requires worldwide military collaboration for developing standardized deployment protocols.

Declaration

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Consent to Publish: Both authors are agreed to publish version of the manuscript in this journal.

Ethical Issues: There are no ethical issues. All data in this paper is publicly available.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Reference

1. Benouachane, H., *Cyber Security Challenges in the Era of Artificial Intelligence and Autonomous Weapons*, in *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*. 2025, CRC Press. p. 24-42.
2. Vrontis, D., et al., *Artificial intelligence, robotics, advanced technologies and human resource management: a systematic review.* Artificial intelligence and international HRM, 2023: p. 172-201.
3. Seixas-Nunes, A., *The Legality and Accountability of Autonomous Weapon Systems: A Humanitarian Law Perspective*. 2022: Cambridge University Press.
4. Anderson, K. and M.C. Waxman, *Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can.* 2013.
5. Quince, S., *The laws surrounding responsibility and accountability of autonomous weapons systems are insufficient: An analysis of legal and ethical implications of autonomous weapons systems.* The Student Journal of Professional Practice and Academic Research, 2021. **3**(1).
6. Malygina, A. and S. Petersburg, *Autonomous Weapon System and Artificial Intelligence: The Problems of Arms Control.*
7. Afzal, J., et al., *Review ofVarious Aspects of Digital Violence.* 2024.
8. Shahid, D. and A. Jamil, *ASSESSING MILITARY NECESSITY OF AUTONOMOUS WEAPONS SYSTEMS (AWS) IN ARMED CONFLICTS: A CASE STUDY OF IRAN-ISRAEL*. Margalla Papers, 2024. **28**(2): p. 95-118.
9. Boothby, W.H., *Weapons and the law of armed conflict*. 2016: Oxford University Press.
10. Chengeta, T., *Measuring autonomous weapon systems against international humanitarian law rules.* JL & Cyber Warfare, 2016. **5**: p. 66.
11. Afzal, J., W. Lumeng, and M. Aslam, *Assessment of tolerance, harmony and coexistence: a study on university students in Government College University, Faisalabad*. Siazga Research Journal, 2022. **1**(1): p. 06-10.
12. Yongmei, C. and J. Afzal, *Impact of enactment of 'the prevention of electronic crimes act, 2016'as legal support in Pakistan.* Academy of Education and Social Sciences Review, 2023. **3**(2): p. 203-212.
13. Veel, P.-E.N., *Incommensurability, proportionality, and rational legal decision-making.* Law & Ethics of Human Rights, 2010. **4**(2): p. 178-228.
14. Horowitz, M.C. and P. Scharre, *MEANINGFUL HUMAN CONTROL inWEAPON SYSTEMS.* 2015.
15. Wallach, W. and C. Allen, *Moral machines: Teaching robots right from wrong*. 2008: Oxford University Press.
16. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024, Springer.
17. Afzal, J., *Legal challenges regarding digital operations*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 23-45.
18. Afzal, J., *Digital Law Enforcement Challenges and Improvement*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 47-78.
19. Afzal, J., *Development of Legal Framework of Digital Laws*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 139-154.
20. Amoroso, D. and G. Tamburrini, *The Human Control Over Autonomous Robotic Systems: What Ethical and Legal Lessons for Judicial Uses of AI?* New Pathways to Civil Justice in Europe: Challenges of Access to Justice, 2021: p. 23-42.
21. Schoenherr, J.R., *Meaningful Human Control of Autonomous Weapons Systems: Translating Functional Affordances to Inform Ethical Assessment and Design*, in *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*. 2025, CRC Press. p. 173-199.
22. Rosert, E. and F. Sauer, *Perspectives for Regulating Lethal Autonomous Weapons at the CCW: A Comparative Analysis of Blinding Lasers, Landmines, and LAWS.* Last modified, 2018.
23. Crootof, R., *A meaningful floor for meaningful human control.* Temp. Int'l & Comp. LJ, 2016. **30**: p. 53.
24. Bode, I., et al., *Prospects for the global governance of autonomous weapons: comparing Chinese, Russian, and US practices.* Ethics and Information Technology, 2023. **25**(1): p. 5.
25. Tzimas, T. and T. Tzimas, *Legal Ramifications of the Use of AWS's-the Role of IHL and Human Rights.* Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective, 2021: p. 167-198.
26. Pollard, M.J., *A Legal Framework for Regulating Autonomous Weapon System Deployments*. 2021, The University Of Buckingham.
27. Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding 'Right to Information'for good governance in Pakistan.* Discover Global Society, 2023. **1**(1): p. 12.
28. Margulies, P., *Making autonomous weapons accountable: command responsibility for computer-guided lethal force in armed conflicts*, in *Research handbook on remote warfare*. 2017, Edward Elgar Publishing. p. 405-442.
29. Verdiesen, I., F. Santoni de Sio, and V. Dignum, *Accountability and control over autonomous weapon systems: a framework for*

comprehensive human oversight. Minds and Machines, 2021. **31**(1): p. 137-163.
30. Sparrow, L.A., et al., *Towards Ethical AI Moderation in Multiplayer Games.* Proceedings of the ACM on Human-Computer Interaction, 2024. **8**(CHI PLAY): p. 1-30.
31. Ahmad, I., A. Haider, and B. Zeb, *In the Name of Nature: The Legal Frontiers of Environmental Preservation.* Journal of Asian Development Studies, 2023. **12**(4): p. 401-411.
32. Haider, A., N. Mathlouthi, and I. Ahmad, *Beyond the Books: Real World Challenges in Implementing Environmental Laws in Pakistan.* Available at SSRN, 2024.
33. Hayes, P., I. Van De Poel, and M. Steen, *Algorithms and values in justice and security.* Ai & Society, 2020. **35**: p. 533-555.
34. Weiss, T.G., *Military-civilian interactions: humanitarian crises and the responsibility to protect*. 2005: Rowman & Littlefield.
35. Docherty, B., *Completing the package: The development and significance of positive obligations in humanitarian disarmament law*, in *Disarmament Law*. 2020, Routledge. p. 57-79.
36. Haider, A., I. Ahmad, and M. Yaseen, *Jus Cogens and the Right to Self-Determination: A Study of its Peremptory Status and Erga Omnes Effects.* 2024.
37. Bradley, M., *Protecting civilians in war: the ICRC, UNHCR, and their limitations in internal armed conflicts*. 2016: Oxford university press.
38. Scheffler, S., *Boundaries and allegiances: Problems of justice and responsibility in liberal thought*. 2002: OUP Oxford.
39. Weigend, T., *Convicting Autonomous Weapons? Criminal Responsibility of and for AWS under International Law.* Journal of International Criminal Justice, 2023. **21**(5): p. 1137-1154.
40. Weigend, T., *Convicting Autonomous Weapons?* 2023.
41. Lay, E. and M. Branlat. *Sending up a FLARE: enhancing resilience in industrial maintenance through the timely mobilization of remote experts.* in *5TH SYMPOSIUM ON RESILIENCE ENGINEERING MANAGING TRADE-OFFS*. 2014.

Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.8

Review

Review of Smart Edible Films and Coatings for Perishable Foods and Future of Smart Packaging

Almas Bibi[1] and Jamil Afzal[2]*

[1]Department of Applied Chemistry, Government College University Faisalabad, Pakistan;

[2]International Islamic University, Malaysia

* Corresponding Email: sirjamilafzal@gmail.com (J. Afzal)

Received: 23 October 2024 / Revised: 26 December 2024 / Accepted: 19 February 2025 / Published online: - 28 February 2025

ABSTRACT

The focus of this review article is smart edible films and coatings and also to elaborates the future of smart packaging for perishable foods. The galaxy of smart packaging is expanding in research and concepts at a quick pace. A number of proposals and preliminary solutions to food preservative issues were produced using recently developed technologies and advanced methods, such as molecular biology and nanotechnology. The study highlights several novel sustainable packaging solutions that must take into account the need to minimize environmental effects, reduce losses, and ensure food safety and quality. Food packaging contributes to waste production in addition to being essential for maintaining food during transportation and storage from farm to table. By lowering the need for chemicals and preservatives, current food packaging systems strive to prolong the shelf life of perishable foods while simultaneously preventing quality deterioration. A number of techniques and strategies, such as oxygen scavenging and antimicrobial technologies, are linked to the creation of modified films.

Keywords*:* Active and Intelligent Packaging; Edible Films; Edible Coatings; Perishable Foods

1. Introduction

By 2050, there will likely be 9.7 billion people on the planet, leading to rapid urbanization and a rise in the need for fresh foods worldwide [1]. A third of all food produced for human consumption, or 1.3 billion tones, is wasted worldwide each year, despite the agro-industry's struggles to meet this rising demand. The majority of losses occur during storage and transportation in the food supply chain (FSC) system, particularly with regard to perishable food items between production and consumption [2]. For example, inadequate storage and transportation circumstances result in damage or uncontrolled natural processes, such as overriding and decreasing shelf-life, wasting 47% of all fruits and vegetables and 12% of meat goods [3]. In addition to these losses, chemical and biological contaminations play a major role. Food preservation is greatly impacted by food packaging, a crucial step in the food manufacturing process [4]. Food packaging serves to keep food isolated from the outside world, preventing microbial contamination and nutrient oxidation brought on by outside influences [5]. Traditional packaging materials' effects on the environment, especially those of single-use plastics, have sparked worries about pollution, resource depletion, and ecosystem damage [6]. Researchers and industry participants have been looking at substitute materials and technologies that provide more environmentally friendly answers to these problems. Making packaging materials out of biopolymers made from renewable resources is one possible approach [7]. A popular carbohydrate polymer derived from crops like corn, wheat, and potatoes, starch has become a viable option because of its renewable nature, biodegradability, and abundance[8].

The primary functions of films and coatings are essential for extending the shelf life of food items [9]. They must prevent UV rays and the movement of substances between the food and the ambient air; they must also serve as a defense against mechanical harm [10]. Antimicrobials, antioxidants, and nutrients are examples of functional/bioactive substances that can be added to stop the growth of bacteria and fungi; Probiotics and other health-promoting microorganisms can improve their nutritional value. It is also pos-

sible to add tastes and aromatic substances as enhancing agents; the finished product should also use biological ingredients and be biodegradable [11]. In the future, more sophisticated uses of smart edible films and coatings are probably going to be produced by continued research and development in this area. Researchers are investigating the use of increasingly complex sensors, like those that can identify certain spoiling components or track foodborne infections. Moreover, these films are performing better thanks to developments in nanotechnology, which are making them thinner, more effective, and able to transport a wider variety of bioactive compounds [12]. In the future of food packaging, smart edible films and coatings will surely be essential as these technologies develop further, tackling issues of environmental sustainability and food security [13].

The aim of this review article is to highlight the use of smart edible films and coatings and provide creative solutions that meet the needs of both the environment and modern consumers. This study will cover;

- The difficulties of the food supply chain in the twenty-first century, these technologies are opening the door for safer, more durable, and environmentally friendly packaging choices by fusing sustainability with active and intelligent features.
- To highlight the advances in nanotechnology, and food safety concerns that are driving the rapid development of smart edible films and coatings in active and intelligent packaging.
- To point out the hindrances related to the creation and application of smart edible films and coatings with consumer acceptance, safety, and regulatory compliance.

2. Edible Films and Coatings

Biopolymers, including proteins, polysaccharides, lipids, and resins, are the primary substances that make films; the qualities of the final films and coatings are significantly influenced by the physical and chemical properties of the biopolymers [14]. Although hydrophilic, hydrophobic, or both can be present in film-forming materials, only water or ethanol can be utilized as solvents to preserve edibility [15]. Proteins are frequently utilized as materials to make films; they are macromolecules with particular molecular structures and amino acid sequences [16]. The amphiphilic nature, electrostatic charges, and conformational denaturation of proteins are what set them apart from other film-forming materials [17]. Heat denaturation, pressure, irradiation, mechanical treatment, acids, alkalis, metal ions, salts, chemical hydrolysis, enzymatic treatment, and chemical crosslinking are all simple ways to alter the secondary, tertiary, and quaternary structures of proteins to produce desired film properties. These processes can regulate the mechanical and physical characteristics of produced coatings and films; animal tissues, milk, eggs, grains, and oilseeds are only a few of the various plant and animal sources from which protein film-forming components can be made [18]. The following Figure 1 is the graphically representation of edible films and coating;

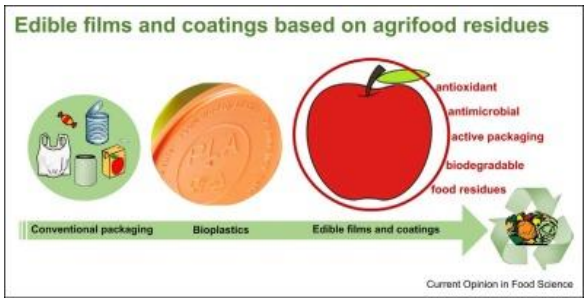

Figure 1: Edible Films and Coating adopted from [19]

Fibers, non-starch carbohydrates, and starch are examples of materials that create polysaccharide films; unlike proteins, which have 20 common amino acids, polysaccharides have simple monomers [20]. However, compared to proteins, polysaccharide structures have far greater molecular weights due to their more complex and unpredictable shape. The majority of carbohydrates have a neutral charge, however, in rare instances; certain gums have a negative charge. Since the neutral carbohydrate structure contains a lot of hydroxyl groups or other hydrophilic moieties, hydrogen bonding is the most important factor in the development and properties of films[21].

2.1. Smart Food Packaging

Four broad categories of food packaging can be distinguished: intelligent, smart, passive, and active packaging [22]. The package's basic and fundamental properties are protected, preserve, and present which are served by a variety of methods. The most common type of packaging to date is the most basic one, which is made of inexpensive materials and doesn't come into contact with the food within. Traditional packaging methods for passive packing include the use of covering materials that have built-in insulating, protecting, or handling properties. For sustainability and food safety, the importance of smart edible films and coatings in food preservation is becoming more widely acknowledged. These cutting-edge materials solve environmental issues related to conventional packing techniques while also extending the shelf life of perishable items [23]. Smart edible films offer a biodegradable substitute that helps to cut down on food waste and packaging pollution by using biopolymers and natural ingredients. In a time when customers are demanding safer, healthier products and sustainability advocates are putting increasing pressure on the global food sector, this move toward more environmentally friendly solutions is crucial. Following Figure 2 is the illustration of smart food packaging;

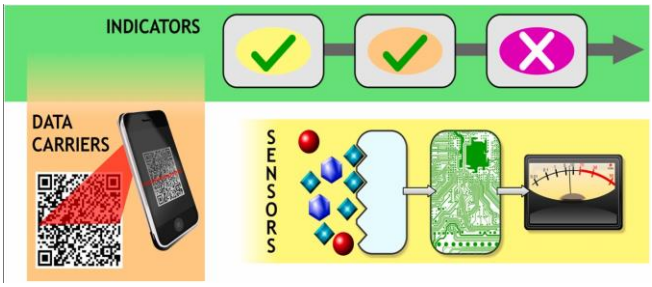

Figure 2: Smart Food Packaging adopted from[24]

The functional capacities of edible films may be improved by the addition of intelligent and active features; bioactive substances with antibacterial and antioxidant properties, such as probiotics or essential oils, can be included in these films [25]. This indicates that these coatings actively support preserving the food's safety and nutritional value in addition to preserving food quality by acting as a barrier against outside influences. Films enhanced with natural preservatives, for example, can stop germs from growing, greatly lowering the risk of foodborne diseases [26]. The function of smart edible films in the circular economy is another crucial element; researchers are looking into making these films out of food industry leftovers, which encourages waste reduction and resource efficiency [27]. For instance, materials made from whey protein or fruit peels not only efficiently use trash but also give the films functional and nutritional improvements. This approach

makes the entire food packaging process more ecologically friendly and aligns with sustainable food development goals.

2.2. Characteristics of Smart Packaging

From a literary perspective, packaging is frequently mentioned as a source of containment that keeps items together and encloses them [28]. However, according to the investigation, there is another possible use for packaging that involves the two-way contact between the consumer and the package that is made possible by enabling communication technology. According to the investigation, the experiences that the packaged product offers the customer have a significant impact on consumer–brand connections[29]. Packaging has the potential to improve these experiences and play a significant role in fostering relationships because it is an integral component of the product. Generally speaking, every package has linguistic, structural, and graphic components, including form, size, color, material, brand, and producer. Additional improved qualities of packaging are produced by applying various design and technology-based advancements to such components. Packaging features are the salient or unique attributes of packaging that allow it to perform its intended duties. Distinct packaging types have distinct features because features are heavily influenced by the kind of product the box holds. A feature of packaging functions is a component that enables the performance of a designated task, activity, or particular role, such as protection or communication.

The packaging industry has recently been forced to address environmental challenges and develop, modify, or design new or existing packaging elements due to mounting environmental pressure [30]. One of the key attributes that packaging needs to have is the ability to interact and communicate with consumers. Additionally, packaging interacts with consumers both inside and outside of the retail setting; that is, packaging communicates with consumers at the point of purchase and at the point of product utilization at home.

3. Types of Smart Edible Films

Food packaging was one of the first commercial applications of nanotechnology in the food industry. About 400–500 goods are already packed using nanoparticles, and almost all of them are employed on a commercial scale. It is anticipated that during the following ten years, nanotechnology would account for 25% of all food packaging. Enhancing the barrier function of food packaging materials is the main goal of nano-packaging, which will limit gas and moisture exchange and manage UV radiation exposure, hence extending product shelf life. For instance, the nanotitanium dioxide plastic addition "DuPont light stabilizer 210," which was introduced by Du Pont, helps to lessen UV damage to foods that are stored in clear containers. The purpose of nanopackaging is to prolong shelf life by facilitating the release of flavors, antioxidants, enzymes, antimicrobials, and nutraceuticals. They acknowledged that this discovery, which was based on research from a UK institute, would completely change the way food is packaged in the future. The microbe-resistant nanoparticles are widely acknowledged to be safe, non-toxic, and helpful for wrapping edible items. The researchers report that ZnO and MnO nanoparticles are essential for destroying microorganisms. Ding and Povey created innovative nanofusion, a novel nanocomposite made up of a variety of functionalized nanoparticles with a size of hundreds of micrometers. Additionally, the capacity to break down liquid components into nanoparticles efficiently targets microorganisms, whose bacteriostatic and antibacterial qualities aid in their death. Based on these results, it is simple to predict what packaging will look like in the near future.

3.1. Active Films and Coatings

The purpose of active films is to absorb or release chemicals that enhance food preservation; these coatings actively fight spoiling agents by containing bioactive substances like enzymes, antioxidants, and antimicrobials [31]. For instance, essential oils with antimicrobial qualities, like cinnamon or oregano, can be used in films to stop the growth of fungi or bacteria. Additionally, by preventing oxidation, these coatings help preserve the food's nutritional value and sensory appeal during long storage times.

3.2. Intelligent Films and Coatings

By including sensors or indicators that identify alterations in the food's surroundings, intelligent films provide real-time food quality monitoring [32]. These films can track variables like microbial activity, gas emissions, and pH levels; they frequently display color changes that signify spoiling; for example, the presence of volatile chemicals created during food spoiling may cause some films to change hue. This lowers waste and enhances food safety by enabling retailers and consumers to visually evaluate the freshness of food.

3.3. Bio-based Films

Polysaccharides, proteins, and lipids are examples of natural, renewable materials used to make bio-based smart edible films; because of these components, the films are biodegradable and provide a sustainable substitute for conventional plastics [33]. These films are frequently made from polysaccharides, such as cellulose and starch, because of their strong moisture and oxygen barriers. Because bio-based films preserve food quality while lowering their environmental impact, they frequently support sustainable packaging objectives.

3.4. Composite Films and Coatings

Composite films improve mechanical strength and barrier qualities by combining several natural or synthetic elements; these films provide better defense against gases and moisture by combining polymers like proteins, polysaccharides, and nanoparticles [34]. Composite films are perfect for packing goods like fresh fruits and vegetables because nanoparticles, such as zinc oxide or silver, are frequently added to increase their antibacterial effectiveness.

3.5. Nanostructured Films and Coatings

Nanotechnology is used in nanostructured films to improve their mechanical and barrier qualities; these coatings' strength, thermal stability, and resistance to moisture and gasses can all be greatly increased by including nanoparticles [35]. Additionally, these coatings have antioxidant and antibacterial properties that enhance food preservation and safety. For even more accurate food quality monitoring, nanostructured coatings can be made to identify rotting indications at the nanoscale level.

3.6. Smart Edible Films

Unlike conventional solutions, intelligent packaging uses natural polysaccharides, which are non-toxic, biocompatible, and biodegradable, to improve functionality [36]. The development and uses of polysaccharide-based intelligent packaging are highlighted in this review, which also covers a variety of sensing techniques for keeping an eye on food attributes like temperature and microbial contamination [32]. In addition to examining present issues and potential future paths, the study highlights the potential of these materials in the food sector. To give consumers information on the quality of food as it is being stored and transported; intelligent food packaging can detect changes in the environment. Because colorimetric pH indicators are inexpensive and easy to use, they have

been used specifically in food-intelligent packaging. Although polysaccharide-based intelligent packaging materials have advanced significantly in recent years, issues including limited mechanical characteristics and moisture sensitivity still exist. These materials require a thorough examination. With an emphasis on polysaccharide-based intelligent packaging systems, different food quality sensing methods and new developments in food packaging, this study examines the most recent research. The opportunities and difficulties these materials face in the market are also covered. Intelligent films used in food packaging:

- pH-Sensitive Films
- Temperature-Responsive Films
- Oxygen Scavenger Films
- Moisture-Responsive Films
- Active Packaging Films

3.7. Antimicrobial films

There are two types of packaging: biodegradable and non-biodegradable; non-biodegradable plastics, such as PET, LDPE, and PP, are widely used because of their strength, affordability, and barrier qualities, but they also present health and environmental hazards [37],[38]. Biodegradable materials are now the main emphasis in order to lessen the environmental impact of packaging due to the increased demand for sustainable packaging. When antimicrobial (AM) agents are included in the polymer film, AM packaging effectively inhibits bacteria. It works better than adding preservatives directly for two reasons: (1) AM agents are released from the film gradually, and (2) there is less chance of inactivation by food ingredients, which can happen when preservatives are introduced directly. Food quality can also be lowered by direct addition, which can alter texture and flavor. Thus, without sacrificing quality, AM packaging extends food safety and shelf life.

3.8. Antioxidant films

Antioxidants, including synthetic kinds like BHT and BHA, are frequently added to polymers to increase food stability and prevent thermal degradation [39]. Problems over the migration of artificial antioxidants into food, however, bring both legal and health problems. Natural antioxidants including tocopherol, plant extracts, and essential oils from plants are being studied as safer substitutes. These natural antioxidants are a promising option for food packaging since they not only stop oxidation but may also enhance the nutritional content of food while it is being stored.

4. Enhancing Food Preservations

Numerous polymers have the ability to create films and are non-toxic, biodegradable, antibacterial, and antioxidant. These characteristics enable their extensive application in the creation of edible films, coatings, and nano-emulsions. However, a number of variables, including the degree of deacetylation, molecular weight, pH, concentration, and origin, affect the biopolymers' functional ability [40]. It is commonly known that the degree of deacetylation and its concentration boost a polymer's antibacterial efficacy. For example, chitosan containing soluble amine groups is created when chitin is deacetylated. The degree of solubility of chitosan is determined by the presence of these soluble amine groups, and it rises as the degree of deacetylation increases. In reaction to stress, plants create secondary metabolites called phenols; they stop oxidation and damage to cells. Polyphenolic substances, including anthocyanin, flavonoids, and phenolic acids, are found in plant extracts. Phenolic and its derivatives are present in these extracts and act as potent antibacterial and antioxidant agents. Because of their ability to scavenge radicals, phenolic compounds function as antioxidants by preventing oxidative chain reactions [41]. When added to coating compositions, the different phenolic elements work in concert to increase the coatings' overall antibacterial and antioxidant capabilities. Phenolics primarily cause membrane instability in microorganisms, which allows them to enter cells and obstruct protein synthesis, ultimately leading to cell death. According to a study, phenolic extracts' antibacterial effectiveness depends on both their concentration and the length of time they are exposed to the test microbe. The following Figure 3 is the example of food preservations mechanism;

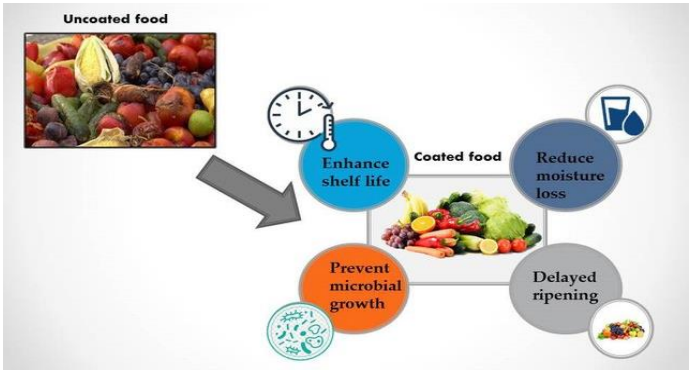

Figure 3: Food Preservations Mechanism adopted from [42]

4.1. Moisture and Gas Control

In order to help regulate the humidity in packaging, moisture absorbers are materials that draw in and hold onto water molecules. These absorbers fall into two categories: moisture removers, which absorb liquids from food, and RH controllers, which control moisture in the packaging headspace (such as desiccants) [43]. Fresh vegetables and meat are frequently covered with moisture removers, which are frequently in the shape of pads or sheets. Although desiccants are frequently employed, superabsorbent composite materials have recently drawn attention because they improve moisture control in food packaging. As a hygroscopic substance, fructose takes in and holds onto moisture for extended periods of time, beginning at 55% relative humidity. It was added to Fruitpad strawberry packaging to improve moisture absorption and decrease weight loss. By regulating in-package humidity, sorbitol, another FDA-approved moisture absorber, increases the shelf life of vegetables like tomatoes and mushrooms. Although they have difficulties breaking down, cellulose derivatives such as carboxymethylcellulose (CMC) are very good at absorbing moisture. Because of their superior moisture-absorbing ability and non-toxic nature, inorganic absorbers such as calcium oxide and silica gel are increasingly frequently utilized [44]. Moisture control films used for food packaging:

- Low-Density Polyethylene (LDPE)
- Polypropylene (PP)
- Polyvinylidene Chloride (PVDC) Coated Films
- Silica Gel or Desiccant Films
- Carboxymethylcellulose (CMC)-Based Films
- Polyamide (Nylon) Films

4.2. Smart films and coatings for fruits

After harvesting, fruits and vegetables continue to be physiologically active, which can cause problems like respiration and water loss and ultimately lower their quality? By decreasing evaporation and respiration, packing materials can have their shelf life increased by reducing moisture and oxygen permeability [45]. It has been demonstrated that edible films work well as barriers, preventing water loss and postponing ripening. These films' capacity to maintain freshness is further improved by the addition of active ingredients like phenolic or essential oils. Because of its ability to

form films and act as antimicrobials, chitosan is frequently used in edible packaging for fresh fruits and vegetables. For example, chitosan films containing 8% galangal oil have been shown to prolong the shelf life of mangoes by 9 days at room temperature while preserving their firmness by slowing respiration and metabolic activity. Furthermore, protein-based films, such as whey protein, are effective barriers against gas diffusion and moisture. Whey protein films containing 0.5% lemongrass essential oil helped preserve polyphenol levels in fresh-cut pears while preserving their firmness during storage [46]. However, the addition of essential oils can affect the fruit's acceptability, indicating that more research is needed to maximize their use.

4.3. Smart films for meat and sea food

During preparation and storage, meat products are susceptible to enzymatic autolysis, lipid oxidation, and microbiological spoiling. Vacuum or nitrogen packaging is frequently employed to address these problems, and edible coatings can be enhanced with natural antioxidants to prevent oxidation [47]. Studies indicate that chitosan films containing essential oils can considerably increase the shelf life of meats. Polysaccharide-based films, especially chitosan, are beneficial because of their antibacterial qualities. Although their significant moisture permeability can be reduced by adding hydrophobic materials, protein-based coatings can enhance mechanical qualities and act as gas barriers. By lowering microbial counts and enhancing barrier qualities, lipid-based films—which are frequently mixed with proteins or polysaccharides—also improve meat quality and shelf life. Recent studies highlight how essential oils, such as garlic oil, can effectively preserve meat products by drastically lowering the number of germs that cause spoiling. Despite being high in proteins and minerals, seafood products—such as fish, shrimp, and shellfish—are extremely susceptible to lipid oxidation and microbial contamination while being stored. Active edible films can be used to decrease lipid oxidation, moisture loss, and microbiological development, improving their quality and prolonging shelf life[48]. For this aim, polysaccharides such as chitosan and alginate have been thoroughly investigated; chitosan has been shown to possess both antibacterial and antioxidant qualities. Research shows that chitosan-based films can suppress contaminants like Listeria monocytogenes on cold-smoked salmon and that adding more antimicrobial agents can increase their effectiveness. For instance, resveratrol-loaded alginate films have been demonstrated to be more effective than standard alginate films at preventing the growth of spoilage microorganisms in rainbow trout that have been stored.

4.4. Smart films for dairy and bakery products

Although dairy products like milk, cheese, and yogurt are rich in nutrients, they are also quite vulnerable to chemical and microbiological deterioration. Active edible films have been created to prevent microbial development and off-flavors, improving their quality and shelf life. Adding antioxidants and antimicrobials, like essential oils, to these films can increase their efficacy [47],[48],[49]. For instance, chitosan-based films containing thyme essential oil can greatly increase the shelf life of Karish cheese by lowering bacterial counts for more than four weeks, while essential oil-loaded alginate films have been demonstrated to shield cheese from microbial contamination and water loss. Products from bakeries rank among the most essential staple meals that people around the world eat on a regular basis. Global sales of bread and other bakery goods will reach approximately $1172.65 billion by 2021, with China alone accounting for over $250.203 billion of the total. By 2027, the global market for bakery products was expected to grow to $457.4 billion; bakery products are among the most important basic foods consumed daily by people throughout the world [50]. By 2021, bread and other bakery products have accumulated about $1172.65 billion in revenue globally, and in China alone, about $250.203 billion had been generated; it was predicted that the global bakery products market would reach $457.4 billion by 2027 [50]. Without preservatives, bakery goods like bread and cakes usually have a short shelf life of three to five days. During this time, their quality is impacted by physical, chemical, and microbiological changes. The industry may suffer financial losses as a result of off-flavors and health hazards brought on by microbial spoiling from bacteria and mold. Although chemical preservatives like calcium propionate and physical preservation techniques like UV radiation and microwaves are employed, they have drawbacks and consumer demand for organic products is growing. To improve food safety, quality, and shelf life, new active and intelligent packaging technologies are being developed; the market for these products is anticipated to expand rapidly [51]. Since consumers may incur additional expenditures, consumer acceptability is critical to the success of innovative packaging methods. Consumer perceptions of active packaging have been the subject of recent research. For instance, consumers' unfamiliarity with antimicrobial packaging led to distrust, although oxygen absorbers were widely accepted in products like bread and pizza.

5. Consumer perception and acceptance

Approximately one-third of the food produced globally each year is wasted. Microbial and oxidative spoilage are the main factors that contribute to food loss and waste, which have significant economic, environmental, and social consequences. Petroleum is the primary source of most food packaging materials due to its affordability, high barrier qualities, and ease of usage. These polymers, however, are not biodegradable and have already given rise to significant environmental concerns. Thus, switching from nonrenewable to renewable materials is the current trend in the packaging sector. In the last phase of the supply chain, packaging is a crucial component of a food product that draws customers and affects their decisions to buy. As a result, it is crucial to educate customers about the advantages of new food packaging, support their use in place of traditional ones, and highlight the packaging cost as part of the product's overall cost.

Prior studies have looked into how food packaging affects the product's ultimate cost. Prior studies have examined food packaging from the viewpoints of producers, businesses, consumers, or technicians. The choice and devotion of consumers to biopolymer films—packaging materials that preserve food because of their useful qualities—is, nevertheless, the subject of relatively little consumer-oriented research. Additionally, biopolymer films are cost-effective for customers and are creative, active, eco-friendly, and sustainable, respectively. The sensory and hedonistic qualities of products are frequently inferred by consumers from their packaging. Additionally, customers frequently get familiar with a product's brand by associating it with its packaging. In this sense, one external factor that is closely linked to brand awareness is container color. Color's impact on customer behavior and product perception is a complex phenomenon with strong roots in consumer research and sensory psychology. Color is a basic emotional reaction generator that has a big impact on customer behavior and purchasing choices. A key element of brand identity that aids in consumer recognition and recall is color. Consumers' sensory experiences and preferences are greatly influenced by a number of elements, including font style, label design, brand name, and contextual appeal.

6. Regulations for smart coatings

Excellent sensory qualities, high barrier qualities, high mechanical strength, high microbiological stability, lack of toxins, safety for human health, ease of production, non-polluting, and affordability are all necessary for a successful edible film. Edible film production is still being done on a lab basis. The commercial success of edible films still faces numerous obstacles.

Edible films have a number of drawbacks over synthetic plastics, including weak mechanical strength (particularly bad elongation), poor gas and liquid resistance, a lack of edibility and biodegradability testing, challenges with processing scale-up, etc. To make the edible films economically successful, it is imperative that these challenges be overcome. The majority of the time, the package is made using traditional methods like extrusion, injection molding, injection stretch blow molding, casting, blown film, thermoforming, foaming, blending, and compounding. This is true even when considering manufacturing techniques for innovative packaging production.

Alternatively, sachets and pads can be placed inside the package, or the active ingredient can be directly integrated into the polymer-based package matrix and/or film. Instead, the primary or secondary packaging can incorporate the intelligent component. To keep up with the advancements in packaging composition and structure, polymer packaging production technologies are also intriguing. The market position of active and intelligent packaging in Europe lags well behind that of other countries, especially the USA, Australia, and Japan, where these items are extensively marketed. Edible sensors for food degradation detection are one kind of sensor that is anticipated to be very successful in the field of intelligent food packaging. These sensors are built entirely of natural and biodegradable materials and do not pose any long-term risks to human health. For instance, a sensor that uses a red cabbage extract as a colorimetric indicator and a pectin matrix has been created. The food industry uses pectin, a naturally occurring polysaccharide that is commercially produced from apples and citrus fruits, to enhance the gelation of food items. An important amount of anthocyanins, specifically cyanidin glycoside derivatives, are present in the red cabbage extract. Anthocyanins are well-known pigments that can detect the presence of amines and change color in response to pH variations.

7. Challenges and Future Trends

The creation and application of smart edible films and coatings are fraught with difficulties related to consumer acceptance, safety, and regulatory compliance. Because these materials come into direct touch with food and may potentially be consumed, it is crucial to ensure their safety. To assess their toxicity, allergen city, and long-term impacts on human health, extensive testing is necessary. For the approval of products that come into contact with food, regulatory agencies enforce strict criteria that can be expensive and time-consuming for businesses to follow. Additionally, businesses looking to market their goods internationally face obstacles due to the diversity of international legislation, which makes compliance more difficult. Another significant obstacle is consumer acceptability. Many customers are cautious of new food technologies, especially those that incorporate edible ingredients, even if creative and sustainable packaging solutions are becoming more and more popular. Widespread adoption may be hampered by worries about the safety of bioactive substances or the possibility that they could change the flavor and texture of food. To increase customer trust and allay worries, education initiatives, and clear labeling are crucial. The commercialization of smart edible films and coatings is hindered by the need for companies to overcome perception and safety concerns in order to gain market acceptability and regulatory approval. Advances in materials science, nanotechnology, and food safety concerns are driving the rapid development of smart edible films and coatings in active and intelligent packaging. The use of nanomaterials, such as nanocellulose, nanoparticles, and nanoemulsions, is one significant development. These materials improve the mechanical and barrier qualities of edible films, increasing their ability to prolong the shelf life of perishable foods. Food preservation is further enhanced by these materials' improved oxygen, moisture, and light barrier qualities. Additionally, nanotechnology makes it possible to create smart coatings that are more sensitive and have improved bioactive qualities, such as antioxidant and antibacterial capabilities, providing a stronger defense against contamination and spoiling. The incorporation of sensor technologies into edible films to create packaging that can continuously check the quality of food is another exciting avenue. In order to improve customer safety and decrease food waste, future research is probably going to concentrate on creating edible films coated with temperature- or pH-sensitive chemicals that can indicate spoiling through color changes. The creation of economical and sustainable biopolymers will also be a top research priority. To create films that are both environmentally benign and practical, scientists are investigating plant-based materials including seaweed, agricultural waste, and other renewable resources. By creating materials that satisfy international safety standards and increasing customer acceptance through open communication and education, research activities will also concentrate on resolving regulatory and safety issues.

8. Conclusion

Smart edible films and coatings are a revolutionary development in the field of intelligent and active packaging for perishable foods. They are a good substitute for conventional packaging techniques because of their capacity to increase food safety, prolong shelf life, and lessen environmental effects. The effectiveness of these packaging options will be further enhanced as research advances by utilizing cutting-edge materials and technologies like sensor integration and nanotechnology. For them to be widely adopted, it is still imperative to overcome issues with consumer acceptance, safety, and regulatory compliance. By emphasizing sustainable practices and informing consumers about the advantages of intelligent edible packaging, the food sector may set the stage for a time when environmental sustainability and food quality are given equal weight.

Declaration

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethical Issues: There are no ethical issues. All data in this paper is publicly available.

Author Contribution Statement: A.B and J.A conceived idea and designed the research; Analyzed interpreted the data and wrote the paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Consent to Publish: Both authors are agreed to publish version of the manuscript in this journal.

References

1. Aryal, J.P., N. Manchanda, and T. Sonobe, *Expectations for household food security in the coming decades: A global scenario*, in *Future foods*. 2022, Elsevier. p. 107-131.
2. Surucu-Balci, E. and O. Tuna, *Investigating logistics-related food loss drivers: A study on fresh fruit and vegetable supply chain.* Journal of Cleaner Production, 2021. **318**: p. 128561.
3. Baneshi, M., et al., *Designing Plant-Based Smart Food Packaging Solutions for Prolonging the Consumable Life of Perishable Foods.* Food Chemistry Advances, 2024: p. 100769.
4. Joardder, M.U., S. Mandal, and M. Masud, *Proposal of a solar storage system for plant-based food materials in Bangladesh.* International Journal of Ambient Energy, 2020. **41**(14): p. 1664-1680.
5. Vasile, C. and M. Baican, *Progresses in food packaging, food quality, and safety—controlled-release antioxidant and/or antimicrobial packaging.* Molecules, 2021. **26**(5): p. 1263.
6. Petkoska, A.T., et al., *Edible packaging: Sustainable solutions and novel trends in food packaging.* Food Research International, 2021. **140**: p. 109981.
7. Fadiji, T., et al., *A review on antimicrobial packaging for extending the shelf life of food.* Processes, 2023. **11**(2): p. 590.
8. Ojogbo, E., E.O. Ogunsona, and T.H. Mekonnen, *Chemical and physical modifications of starch for renewable polymeric materials.* Materials today sustainability, 2020. **7**: p. 100028.
9. Jafarzadeh, S., et al., *Application of bio-nanocomposite films and edible coatings for extending the shelf life of fresh fruits and vegetables.* Advances in Colloid and Interface Science, 2021. **291**: p. 102405.
10. Koutchma, T., *Ultraviolet light in food technology: principles and applications*. 2019: CRC press.
11. SÁ, A.G.A., et al., *A review on enzymatic synthesis of aromatic esters used as flavor ingredients for food, cosmetics and pharmaceuticals industries.* Trends in Food Science & Technology, 2017. **69**: p. 95-105.
12. Zhang, L., et al., *A comprehensive review on natural bioactive films with controlled release characteristics and their applications in foods and pharmaceuticals.* Trends in Food Science & Technology, 2021. **112**: p. 690-707.
13. Luo, Y., Q. Wang, and Y. Zhang, *Biopolymer-based nanotechnology approaches to deliver bioactive compounds for food applications: a perspective on the past, present, and future.* Journal of Agricultural and Food Chemistry, 2020. **68**(46): p. 12993-13000.
14. Nussinovitch, A., *Biopolymer films and composite coatings*, in *Modern biopolymer science*. 2009, Elsevier. p. 295-326.
15. Hassan, B., et al., *Recent advances on polysaccharides, lipids and protein based edible films and coatings: A review.* International journal of biological macromolecules, 2018. **109**: p. 1095-1107.
16. Hammann, F. and M. Schmid, *Determination quantification of molecular interactions in protein films: A review.* Materials, 2014. **7**(12): p. 7975-7996.
17. Wang, K., et al., *Principles and applications of spectroscopic techniques for evaluating food protein conformational changes: A review.* Trends in Food Science & Technology, 2017. **67**: p. 207-219.
18. Han, J.H., *Edible films and coatings: a review.* Innovations in food packaging, 2014: p. 213-255.
19. Gaspar, M.C. and M.E. Braga, *Edible films and coatings based on agrifood residues: a new trend in the food packaging research.* Current opinion in food science, 2023. **50**: p. 101006.
20. Habte-Tsion, H.-M. and V. Kumar, *Nonstarch polysaccharide enzymes—general aspects*, in *Enzymes in human and animal nutrition*. 2018, Elsevier. p. 183-209.
21. Das, A., et al., *A comprehensive review on recent advances in preparation, physicochemical characterization, and bioengineering applications of biopolymers.* Polymer Bulletin, 2023. **80**(7): p. 7247-7312.
22. Ghoshal, G., *Recent trends in active, smart, and intelligent packaging for food products*, in *Food packaging and preservation*. 2018, Elsevier. p. 343-374.
23. Nilsen-Nygaard, J., et al., *Current status of biobased and biodegradable food packaging materials: Impact on food quality and effect of innovative processing technologies.* Comprehensive reviews in food science and food safety, 2021. **20**(2): p. 1333-1380.
24. Azeredo, H.M. and D.S. Correa, *Smart choices: Mechanisms of intelligent food packaging.* Current Research in Food Science, 2021. **4**: p. 932-936.
25. Pavli, F., et al., *Probiotic incorporation in edible films and coatings: Bioactive solution for functional foods.* International Journal of Molecular Sciences, 2018. **19**(1): p. 150.
26. Baptista, R.C., C.N. Horita, and A.S. Sant'Ana, *Natural products with preservative properties for enhancing the microbiological safety and extending the shelf-life of seafood: A review.* Food research international, 2020. **127**: p. 108762.
27. Versino, F., et al., *Sustainable and bio-based food packaging: A review on past and current design innovations.* Foods, 2023. **12**(5): p. 1057.
28. Paine, F.A. and H.Y. Paine, *A handbook of food packaging*. 2012: Springer Science & Business Media.
29. Soroka, W., *Illustrated glossary of packaging terminology*. 2008: DEStech Publications, Inc.
30. Vanderroost, M., et al., *Intelligent food packaging: The next generation.* Trends in food science & technology, 2014. **39**(1): p. 47-62.
31. Benbettaïeb, N., F. Debeaufort, and T. Karbowiak, *Bioactive edible films for food applications: Mechanisms of antimicrobial and antioxidant activity.* Critical reviews in food science and nutrition, 2019. **59**(21): p. 3431-3455.
32. Perera, K.Y., et al., *Seaweed polysaccharide in food contact materials (active packaging, intelligent packaging, edible films, and coatings).* Foods, 2021. **10**(9): p. 2088.
33. Martins, V.F., et al., *Recent highlights in sustainable bio-based edible films and coatings for fruit and vegetable applications.* Foods, 2024. **13**(2): p. 318.
34. Cazón, P. and M. Vázquez, *Mechanical and barrier properties of chitosan combined with other components as food packaging film.* Environmental Chemistry Letters, 2020. **18**(2): p. 257-267.
35. Mihindukulasuriya, S. and L.-T. Lim, *Nanotechnology development in food packaging: A review.* Trends in Food Science & Technology, 2014. **40**(2): p. 149-167.
36. Kontogianni, V.G., et al., *Innovative intelligent cheese packaging with whey protein-based edible films containing spirulina.* Sustainability, 2023. **15**(18): p. 13909.
37. Shaikh, S., M. Yaqoob, and P. Aggarwal, *An overview of biodegradable packaging in food industry.* Current Research in Food Science, 2021. **4**: p. 503-520.
38. Ivonkovic, A., et al., *Biodegradable packaging in the food industry.* J. Food Saf. Food Qual, 2017. **68**(2): p. 26-38.
39. Sanches-Silva, A., et al., *Trends in the use of natural antioxidants in active food packaging: A review.* Food Additives & Contaminants: Part A, 2014. **31**(3): p. 374-395.
40. Kumirska, J., et al., *Biomedical activity of chitin/chitosan based materials—influence of physicochemical properties apart from molecular weight and degree of N-acetylation.* Polymers, 2011. **3**(4): p. 1875-1901.
41. Santos-Sánchez, N.F., et al., *Antioxidant compounds and their antioxidant mechanism.* Antioxidants, 2019. **10**: p. 1-29.
42. Shahbaz, M.U., et al., *Natural plant extracts: an update about novel spraying as an alternative of chemical pesticides to extend the postharvest shelf life of fruits and vegetables.* Molecules, 2022. **27**(16): p. 5152.
43. Gaikwad, K.K., S. Singh, and A. Ajji, *Moisture absorbers for food packaging applications.* Environmental Chemistry Letters, 2019. **17**(2): p. 609-628.
44. Yadav, S. and P.K. Dutta, *Moisture-Absorbent Food Packaging Systems and the Role of Chitosan.* Smart Food Packaging Systems: Innovations and Technology Applications, 2024: p. 169-193.
45. Popović, S.Z., et al., *Biopolymer packaging materials for food shelf-life prolongation*, in *Biopolymers for food design*. 2018, Elsevier. p. 223-277.
46. Galus, S., et al., *The effect of whey protein-based edible coatings incorporated with lemon and lemongrass essential oils on the quality attributes of fresh-cut pears during storage.* Coatings, 2021. **11**(7): p. 745.
47. Moura-Alves, M., et al., *Antimicrobial and antioxidant edible films and coatings in the shelf-life improvement of chicken meat.* Foods, 2023. **12**(12): p. 2308.
48. Umaraw, P., et al., *Edible films/coating with tailored properties for active packaging of meat, fish and derived products.* Trends in Food Science & Technology, 2020. **98**: p. 10-24.
49. Martín-Belloso, O., M.A. Rojas-Graü, and R. Soliva-Fortuny, *Delivery of flavor and active ingredients using edible films and coatings.* Edible films and coatings for food applications, 2009: p. 295-313.
50. Qian, M., et al., *A review of active packaging in bakery products: Applications and future trends.* Trends in Food Science & Technology, 2021. **114**: p. 459-471.
51. Sohail, M., D.-W. Sun, and Z. Zhu, *Recent developments in intelligent packaging for enhancing food quality and safety.* Critical reviews in food science and nutrition, 2018. **58**(15): p. 2650-2662.