International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Cyber-Sociology: Understanding Risk And Vulnerability In The Digital Era.

Malay Maity[1], Ranjan Banerjee[2], Misha Samanta[3]

Department Of Computer Science & Engineering Brainware University, Barasat, Kolkata – 125 Pincode:721137 West Bengal, India

Email Id: maitymalay27747@gmail.com, rbkpccst@gmail.com, mishasamanta47@gmail.com

ABSTRACT

This research investigates the sociological dimensions of cybersecurity and digital vulnerability, examining how the ongoing digital transformation interacts with the social structures that define cyberspace. The central premise suggests that digital risks are not merely technical anomalies but are deeply embedded social phenomena emerging from the confluence of technological disparities, collective digital awareness, and human behavioral patterns. As society becomes increasingly reliant on digital media, the resulting expansion of the digital divide has given rise to sophisticated cyberthreats that challenge the security of individuals, institutional integrity, and state sovereignty.To analyze these dynamics, the study synthesizes three primary theoretical frameworks: Ulrich Beck's Risk Society, which provides a lens for the production of digital hazards in late modernity; Erving Goffman's Symbolic Interactionism, which elucidates the management of digital identity within networked spaces; and Manuel Castells's Network Society, which highlights the restructuring of power and the intensification of digital vulnerability. The analysis reveals that vulnerability is primarily driven by deficient security awareness, the digital divide, and a lack of robust institutional governance. Ultimately, the research positions cybersecurity as an essential pillar of broader social security, asserting that a sociological understanding is a prerequisite for mitigating digital risk and ensuring societal stability in a hyper-connected era.

Keywords: *cybersecurity, digital age, social vulnerability, digital society, cyber risk.*

Introduction:

In the modern era, the digital revolution has fundamentally restructured the human experience, permeating every sector from global economics and political discourse to the nuances of education and interpersonal communication. This shift has established cyberspace as the foundational infrastructure of contemporary society, where technological platforms now mediate daily interactions and govern our relationship with the world. Consequently, cybersecurity has transitioned from a niche technical concern to a pivotal societal priority. At its essence, protecting data and digital identities is a social endeavor, deeply intertwined with human behavior, collective awareness, and the way individuals perceive risk within a virtual environment. A sociological perspective is therefore vital, as it illuminates the social frameworks that produce digital hazards and the mechanisms that perpetuate vulnerability across different populations.As the boundaries between the physical and virtual worlds blur, cyberspace has evolved into a landscape that profoundly reshapes social bonds. However, this openness has introduced multifaceted threats that transcend mere malware; we now face digital violence, systemic extortion, and the strategic manipulation of information. These hazards do not impact all users uniformly. Instead, risk exposure is dictated by social, cultural, and cognitive disparities. The concept of "social vulnerability" is critical here, as factors such as age, gender, education, and socioeconomic status directly influence an individual's capacity for self-protection.The necessity of a sociological approach to cybersecurity is driven by two primary challenges. First, the velocity of technological advancement often outpaces the public's ability to acquire necessary protective skills. Second, our total systemic reliance on digital media means that any technical breach carries profound implications for collective social safety. The prevalence of socially-driven attacks—such as social engineering, phishing, and targeted digital harassment—demonstrates that cyber risk is as much about cultural and social dynamics as it is about software vulnerabilities. True security cannot be achieved through encryption alone; it requires the cultivation of a responsible digital culture and heightened social consciousness.This perspective is particularly relevant in rapidly digitizing regions, such as the Arab world, where the surge in internet adoption has not always been met with equivalent security literacy or robust institutional protections. Understanding why certain demographics remain more susceptible to exploitation is both a scientific and a civic requirement. By examining how risks emerge from within the social fabric itself, we can better understand the complex interaction between the individual and the digital domain.This article provides an in-depth sociological analysis of

cybersecurity, interpreting the emerging risks and the social vulnerabilities they generate. By moving beyond a purely technical lens, this study treats cybersecurity as a structural issue shaped by societal values and interaction patterns. Ultimately, this analysis seeks to build a comprehensive knowledge framework that encourages a holistic social approach to digital safety, offering solutions that transcend traditional technical boundaries to ensure stability in a hyper-connected world.

Problem Statement

The contemporary global landscape is undergoing a radical metamorphosis catalyzed by the digital revolution and the ubiquitous integration of technology into the fabric of daily existence. Cyberspace has evolved far beyond its origins as a technical medium or a simple communication tool; it has matured into a fundamental structural pillar of social life. It now dictates the modalities of human interaction, the architecture of personal relationships, and the generation of modern cultural symbols. Within this framework, individual behaviors are recalibrated, digital personas are constructed, and transboundary social networks are established, effectively merging the physical and virtual realms.

As the social and digital spheres become inextricably linked, there is a critical need to redefine **cybersecurity**. It must be viewed not merely as a technical firewall protecting infrastructure, but as a complex social phenomenon deeply rooted in cultural frameworks, collective ethics, and societal consciousness.

The Socialization of Digital Risk

The accelerated pace of technological innovation has birthed a new genus of digital hazards that transcend traditional hacking. These risks often manifest as:

- **Social Engineering:** Exploiting human psychology and trust rather than software vulnerabilities.
- **Systemic Digital Violence:** The rise of online harassment and targeted victimization.
- **Privacy Erosion:** The commodification and exploitation of personal data.

These threats render cybersecurity a quintessentially sociological concern. Vulnerability is not distributed randomly; it is directly correlated with an individual's cognitive preparedness, digital literacy, and socioeconomic standing. This mirrors Ulrich Beck's "Risk Society" (1992), which argues that modern technological progress inherently generates new forms of systemic risk that become inseparable from daily social reality. In this sense, cybersecurity is a co-production of technical protocols and the prevailing social culture.

Cyber Vulnerability and Social Disparity

Digital vulnerability frequently serves as an extension of traditional social inequality. An individual's susceptibility to cyber threats is often dictated by:

1. **Educational Attainment:** Influencing the ability to discern misinformation.
2. **Economic Status:** Determining access to secure hardware and software.
3. **Demographic Variables:** Including gender and generational gaps in technical fluency.

Arab scholar **Nabil Ali (2003)** identified that while digital adoption in Arab societies has been rapid, it has often lacked a parallel development of a resilient "digital culture." This disconnect hinders the ability of individuals to engage with cyberspace consciously and safely, proving that digital threats are anchored more in human perception and cognitive readiness than in the machines themselves.

Cybersecurity as Social Security

The rationale for investigating this intersection lies in the fact that cybersecurity is now a prerequisite for **societal security**. Social trust—the bedrock of community cohesion—is under constant assault from digital impersonation, deception, and the spread of inflammatory misinformation. Furthermore, historically marginalized or vulnerable groups, such as children and the elderly, face amplified risks due to technical knowledge gaps.

Consequently, this study addresses a pivotal central question:

How do existing social structures and digital cultures actively contribute to the production and reproduction of cyber vulnerability within the contemporary digital society?

By framing the issue this way, we can re-evaluate the role of primary social institutions—such as the family, the educational system, and the media—as vital agents in fostering digital awareness. This perspective allows for the construction of a societal framework capable of navigating the threats of the digital age through the following hypotheses:

Hypothesis One (H1): The Digital Divide and Socio-Technical Susceptibility

Hypothesis One (H1) posits that the digital divide serves as a primary catalyst for increasing an individual's exposure to cyber vulnerability within the contemporary digital society. This premise suggests that disparities in access to advanced technology, combined with a deficiency in critical digital competencies, create a stratified landscape of risk where specific social groups are rendered disproportionately susceptible to digital exploitation and victimization.

The Multi-Dimensional Nature of the Digital Divide

In the context of this study, the digital divide is not viewed merely as a binary of "haves" and "have-

nots" regarding hardware. Instead, it is analyzed as a multi-layered barrier that includes:

- **Access Disparity:** Unequal distribution of high-speed connectivity and secure computing devices, which often forces marginalized groups to rely on insecure public networks or outdated, vulnerable hardware.
- **The Skills Gap:** A lack of "cyber-hygiene" and technical literacy that prevents users from identifying sophisticated threats such as phishing, social engineering, or data harvesting.
- **Cognitive Vulnerability:** The inability to critically evaluate the legitimacy of digital content, making individuals more prone to misinformation and predatory digital schemes.

Mechanism of Exploitation

The hypothesis argues that as society migrates its essential functions—banking, governance, and social interaction—to the cloud, those on the wrong side of the digital divide are forced to navigate a high-risk environment without the necessary "protective armor." This lack of proficiency does not just result in exclusion; it invites predatory exploitation. Cyber adversaries frequently target demographics with lower technical literacy, recognizing that these individuals possess fewer defensive resources and are less likely to employ multi-factor authentication or encrypted communication channels.

Sociological Implications

From a sociological standpoint, this hypothesis suggests that digital vulnerability is a reproduction of traditional social inequality. Socioeconomic status, geographic location, and educational attainment directly correlate with an individual's "digital resilience." Consequently, the digital divide acts as a force multiplier for risk, transforming a lack of technological resources into a profound threat to personal, financial, and social security. By validating this hypothesis, the study emphasizes that cybersecurity cannot be achieved through technical patches alone but requires the systemic closure of the digital and educational gap to protect the most vulnerable segments of the networked society.

Hypothesis Two (H2): Social Awareness as a Determinant of Digital Resilience

Hypothesis Two (H2) asserts that the deficiency in security awareness, viewed as a critical social factor, significantly amplifies an individual's vulnerability within the virtual ecosystem. This proposition suggests that technical safeguards are often rendered ineffective by unconscious behavioral patterns—such as the mismanagement of credentials or engagement with malicious links—thereby intensifying the risk profile for socially and technologically marginalized groups.

The Human Element as a Structural Weakness

This hypothesis shifts the focus from hardware vulnerabilities to the human-centric dimensions of cybersecurity. It posits that digital risk is frequently the result of a "social vacuum" where users interact with complex systems without a foundational understanding of the threat landscape. Within this framework, security awareness is treated not just as technical knowledge, but as a social competency that dictates how safely an individual navigates the networked world.

Behavioral Drivers of Risk

The study argues that high-risk behaviors are often deeply rooted in social habits and a lack of perceived consequence. Key behavioral factors include:

- **Trust Over-Extension:** The tendency to trust digital personas or "urgent" communications, which leads to the clicking of suspicious links or the downloading of malicious attachments.
- **Credential Negligence:** The habitual use of weak passwords or the sharing of sensitive authentication data across social circles, reflecting a lack of "digital boundary" awareness.
- **Cognitive Dissonance:** A disconnect where users recognize general cyber threats but believe themselves to be immune, leading to a relaxation of protective behaviors in daily digital routines.

Socio-Cultural Vulnerability

The hypothesis further suggests that certain demographics—such as the elderly, children, or those new to the digital space—are at a higher risk because they lack the cultural intuition required to recognize digital deception. In these instances, the absence of security awareness acts as a catalyst for social engineering, where attackers bypass sophisticated encryption by simply exploiting the user's lack of skepticism or "cyber-hygiene."

Conclusion of the Premise

Ultimately, H2 proposes that cybersecurity is a social construct built on the foundation of collective consciousness. If a society lacks a robust, pervasive culture of security awareness, no amount of technical infrastructure can fully mitigate the risk of exploitation. By exploring this hypothesis, the research seeks to demonstrate that strengthening the "human firewall" through education and social intervention is as vital to national security as the development of advanced software defenses.

Hypothesis Three (H3): The Role of Social Institutions in Mitigating Digital Risk

Hypothesis Three (H3) proposes that **primary social institutions**—specifically the family, the

educational system, and the media—serve as the decisive frontline in the reduction of digital vulnerability. This premise suggests that the mitigation of cyberthreats is not a solitary technical task but a collective social responsibility. By establishing a coordinated "institutional synergy," these pillars of society can effectively disseminate digital literacy and cultivate a state of collective resilience that shields individuals from the evolving hazards of the virtual world.

The Institutional Architecture of Defense

This hypothesis views social institutions as the primary architects of a user's "digital conscience." Their influence is categorized as follows:

- **The Family Unit:** As the foundational site of socialization, the family is responsible for establishing early "digital boundaries" and ethical online behavior. Parental guidance and intergenerational knowledge transfer act as the first layer of defense against grooming, cyberbullying, and data oversharing.
- **Educational Systems:** Schools and universities transition from mere providers of information to hubs of **cyber-civics**. By integrating security awareness into the curriculum, education systems transform passive technology users into critical thinkers capable of identifying social engineering and technical manipulation.
- **The Media Landscape:** Both traditional and digital media serve as the "public alert system." Their role involves demystifying complex technical threats and fostering a national discourse on digital safety, ensuring that security awareness reaches all socioeconomic strata.

Significance of the Study

The importance of this research lies in its departure from traditional technical frameworks, offering a profound understanding of the human and societal elements of the virtual world:

- **Sociological Recontextualization of Risk:** It uncovers the sociological dimensions of cybersecurity by examining the symbiotic link between technology and social architecture. The study clarifies the process by which technical vulnerabilities evolve into profound social risks that jeopardize the stability of both the individual and the collective.
- **Deciphering Social Determinants:** It illuminates how demographic and social variables—including age, academic attainment, and socioeconomic standing—dictate an individual's level of risk perception. This helps explain why different social strata possess varying degrees of agency in safeguarding their digital identities.
- **The Nexus of Cyber and Social Security:** The research establishes a critical connection between digital integrity and broader **social security**, demonstrating that virtual breaches can manifest as tangible threats to the physical and psychological safety of society.
- **Defining Digital Vulnerability:** It expands the academic discourse by categorizing digital vulnerability as a modern form of social hazard, one that necessitates a holistic, multidimensional strategy for mitigation.

Objectives of the Study

This research seeks to achieve several key academic and practical milestones:

- **Sociological Analysis of the Cyber Landscape:** To investigate the cyber phenomenon through a sociological lens, understanding the intricate ways cybersecurity is woven into the social structures and digital shifts of the modern era.
- **Categorization of Socially Impactful Threats:** To pinpoint the specific varieties of cyberthreats that most aggressively target individuals and to analyze how these hazards reshape interpersonal dynamics and social engagement within digital environments.
- **Examination of Social Variables:** To critically evaluate how factors such as generational gaps, educational backgrounds, and social status contribute to the existing disparities in cybersecurity awareness among diverse populations.
- **Assessment of Defensive Competencies:** To gauge current levels of public security consciousness and measure the practical capacity of individuals to defend their sensitive data and digital personas within an increasingly networked service economy.

The Conceptual and Theoretical Framework

The Concept of Cybersecurity

Cybersecurity is a defining pillar of modern digital existence. While technically defined as the suite of protocols and tools used to defend networks and data from intrusion, a sociological interpretation views it as a determinant of societal stability. Whitman and Mattord (2022) describe it as a combination of policy and technical means to protect information assets, while Singer and Friedman (2014) emphasize that it has evolved into a theater of national security and social conduct.From a digital sociology

standpoint, cybersecurity is about the influence of technology on social trust and power. Control over information flows constitutes a form of modern power (Castells, 2010). Thus, security serves as a regulatory mechanism for virtual spaces. As Kello (2017) notes, cyber-attacks have lasting consequences on political and social ties, while Bayuk (2011) asserts that true security requires an understanding of digital behavior rather than just technical infrastructure. Ultimately, the human factor remains the primary vulnerability; daily user decisions dictate the level of risk, making cybersecurity a deeply interwoven socio-technical system.

The Concept of the Digital Society

The digital society marks a phase of social evolution where technology mediates every facet of life—from labor and education to personal entertainment. Debray (2017) characterizes it as a structure where digital media reshapes production and interaction patterns. Unlike traditional societies, it relies on the flow of information rather than physical borders. In this "network society," power is derived from communication capacity rather than material wealth (Castells, 2010).Sociologically, this society involves a radical reorganization of relationships, giving rise to concepts like digital citizenship and the immaterial economy. Lévy (1999) describes this as a "knowledge society" that creates new virtual spaces for belonging. While Ritzer (2021) highlights the "digitally empowered individual" who participates in content creation, Fuchs (2014) cautions that these platforms also enable new forms of surveillance and behavioral regulation. Consequently, the digital society is a dual space of unprecedented freedom and subtle domination, where cybersecurity is essential for maintaining cohesion.

The Concept of Cyber Vulnerability

Cyber vulnerability refers to the degree to which individuals or organizations are susceptible to digital harm, influenced by a blend of technical and behavioral factors. Cavelty (2015) defines it as any weakness—technical or human—that allows for a breach. This vulnerability is exacerbated by a "dependency gap," where society's reliance on technology outpaces its ability to secure it (Clarke & Knake, 2010).

Boyes (2019) categorizes this vulnerability into three distinct tiers:

1. **Technical:** Flaws in hardware or software.
2. **Human:** Deficiencies in awareness and susceptibility to deception.
3. **Institutional:** Inadequate organizational policies and structures.

With research showing that the human factor accounts for approximately 70% of security breaches (Anderson, 2020), vulnerability is clearly a social issue. In societies with weak digital cultures, this vulnerability is heightened by the spread of disinformation and fraud, which erodes trust in the digital domain (Lewis, 2018). Therefore, cyber vulnerability is a key sociological metric that explains why risk levels vary across different demographics and how the digital divide continues to be reproduced.

Second: Categories of Digital Risk

Digital risks represent a multifaceted challenge in the wake of rapid technological shifts. They exist at the intersection of technical, behavioral, and structural threats. These hazards can be categorized based on their origins and their specific impacts on the individual and the state.

Technical Risks

These involve direct attacks on the integrity of hardware and software. Examples include malware, viruses, and Distributed Denial-of-Service (DDoS) attacks, alongside the exploitation of "zero-day" vulnerabilities (Reddy & Ugander Reddy, 2014). For institutions relying on outdated or poorly defended systems, these risks can lead to catastrophic data loss and service failures.

Behavioral Risks

Rooted in human action, these risks stem from how users engage with the digital world. Actions such as revealing sensitive data, accepting friend requests from strangers, or clicking unverified links often result from low security awareness. Research suggests these behaviors significantly increase the probability of falling victim to cyberbullying or electronic extortion (Evans et al., 2016).

Organizational Digital Risks

Institutions face specific vulnerabilities when they lack cohesive internal security strategies or robust policies. This includes poor management of employee credentials and a lack of emergency response protocols (Mansouri, 2022). Such negligence can lead to the collapse of public services and the loss of critical strategic information.

Sociodigital Risks

This category focuses on the erosion of social fabric through digital means. It includes the viral spread of misinformation, social polarization, and the formation of online pressure groups. These factors significantly impact communal trust and the mental well-being of users (Bada & Nurse, 2019).

Third: Social Determinants of Digital Vulnerability

Digital vulnerability is a social construct shaped by the interaction between technology and human society. The following factors determine how susceptible a group or individual is to digital harm:

1. Deficiencies in Digital Culture and Awareness

A primary driver of vulnerability is the lack of "cyber-hygiene." Many users do not know how to manage passwords or identify fraudulent communications. As Al-Hammadi (2020) notes, this knowledge gap leads to reckless information

sharing, making users easy targets for cyber-attacks and harassment.

2. Socioeconomic Inequality

Vulnerability is often a reflection of the "digital divide." Those with lower incomes or limited education often lack access to secure technology or the training required to use it safely. This highlights that digital vulnerability is deeply rooted in the existing socioeconomic hierarchy (Mansouri, 2022).

3. Unconscious Use of Social Media

The habit of "oversharing" on social platforms significantly elevates risk. Many young users publicly broadcast their private lives, facilitating identity theft and extortion (Marwick & Boyd, 2014). This makes social interaction patterns a direct catalyst for vulnerability.

Strategic Conclusions

The sociological evaluation of this study confirms that cybersecurity has evolved into a strategic pillar for the stability of the digital era, spanning the protection of individual citizens, public institutions, and critical network architectures. Cultivating a robust digital culture, elevating public security consciousness, and mobilizing the influence of primary social institutions—namely the family, the school, and the media—serve as the indispensable foundation for minimizing digital susceptibility.Furthermore, contemporary research within the Algerian context highlights that the lack of rigorous institutional governance over digital assets creates a "security vacuum." This vulnerability in public services does not merely pose a technical risk but threatens the equilibrium of the entire social body.From this viewpoint, cybersecurity is a holistic social phenomenon that demands an integrated response, weaving together technology, legislation, culture, and social structure. Establishing a resilient and secure digital society requires a multifaceted approach focused on:

- **Cultural Fortification:** Embedding digital safety into the collective consciousness.
- **Identity Agency:** Empowering individuals with the specific skills necessary to defend their virtual personas.
- **Closing the Technological Divide:** Eliminating the socioeconomic gaps that lead to unequal protection.
- **Institutional Governance:** Implementing clear, enforceable policies and frameworks within the public and private sectors.

In finality, this research demonstrates that digital vulnerability is more a product of social architecture and digital culture than of technology in isolation. Any effort to mitigate cyber risks that ignores these human and cultural dimensions is destined to be inadequate. Cybersecurity is a fundamental social and strategic metric; it reflects a society's maturity in organizing itself, fostering mutual trust, and maintaining the integrity of its networks. The digital future of modern societies depends on a seamless integration of technical defense with social awareness and institutional oversight to ensure that the virtual world remains a secure, stable, and sustainable space for human interaction.

Final Synthesis and Recommendations

Conclusion

The findings of this study demonstrate that digital space is no longer a purely technical realm; it has evolved into a social landscape where threats have direct and profound societal consequences. Beyond mere data theft, cybervulnerability now manifests as the erosion of interpersonal trust, the precarious management of digital personas, and fundamental shifts in the patterns of digital social interaction (Alharbi & Tassaddiq, 2021). The research highlights that disparities in digital literacy, socioeconomic status, and security awareness lead to a fragmented landscape of vulnerability, where specific demographics are disproportionately exposed to exploitation and extortion (Khan et al., 2023).

Analysis through the lens of established sociological frameworks confirms these dynamics:

- **Beck's Risk Society:** Illustrates how digital threats are "socially produced" risks that often exceed the defensive capacities of individual users (Beck, 1992).
- **Goffman's Symbolic Interactionism:** Reveals that inadequate protection of digital identities leads to "fragile" social fronts, complicating the presentation of self in virtual spaces.
- **Castells's Network Society:** Highlights that the structural complexity of contemporary digital networks inherently expands the surface area for vulnerability and redistributes power among traditional and non-traditional actors (Mahmood et al., 2024).

Both international and regional research—specifically within the Algerian context—support the conclusion that a weak digital culture and a lack of institutional governance threaten the overall stability of the networked society. Cybersecurity must therefore be understood as a social pillar, requiring multidimensional strategies that integrate technical knowledge with cultural and institutional engagement.

Strategic Recommendations

To enhance cybersecurity and reduce systemic digital vulnerability, the following actions are recommended:

1. **Cultivating a Digital Prevention Culture:** Adopt community-based initiatives focused on "digital hygiene," specifically teaching individuals to identify disinformation and navigate privacy settings (Mahmood et al., 2024).

2. **Supporting Vulnerable Demographics:** Develop specialized support platforms and guidance frameworks for high-risk groups, including women, children, and older adults, to ensure their safe inclusion in the digital economy.
3. **Cross-Sector Collaboration:** Establish formal information-sharing policies between the public and private sectors to facilitate rapid response to emerging digital threats (Khan et al., 2023).
4. **Institutional Risk Assessment:** Implement periodic, systematic audits of both technical infrastructure and human behavior patterns to proactively identify points of failure.
5. **Integrating Digital Education:** Embed cybersecurity and digital ethics into formal academic curricula from an early age, equipping future generations with the "social immunity" needed for the digital age (Alharbi & Tassaddiq, 2021).
6. **Sociological Research Expansion:** Promote interdisciplinary research that bridges the gap between technical security and the social sciences to develop solutions that address the human root of vulnerability.
7.

References

Reference-1
Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023
Reference-2
Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.
Dahdal, A. M., & Abdel Ghafar, A. (2025). The digital silk road: "Tech-diplomacy" as a paradigm for understanding technological adoption and emerging digital regulations in MENA. *Asian Journal of Law and Society*, 1–26. https://doi.org/10.1017/als.2024.30
Reference-3
Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*, *37*, 214–244. https://doi.org/10.1057/s41284-023-00375-4
Reference-4
Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing cybersecurity challenges in times of crisis: Extending the sociotechnical systems perspective. *Applied Sciences*, *14*(24), 11610. https://doi.org/10.3390/app142411610
Reference-5
A Study on Cyber Defence Curse for Online Attackers
R Banerjee, R Sahu, TA Gazi - Strengthening Industrial Cybersecurity to Protect …, 2024
Reference-6
Exploring The Intersection of AI and Cybersecurity
M Maity
Reference-7
Unweaving the Cyber Attack-The Cyber Kill Chain Analysis
R Banerjee, D Mukherjee, PS Nayak, S Nath, MM Islam
Reference-8
Shattering the Cyber Attack Paradigm: A Defense Study
R Banerjee, D Mukherjee, S Sarkar
Reference-9
A Survey on Cloud Security Issues and Techniques
S Subashini, V Kavitha
Reference-10
Zero Trust Architecture
S Rose, O Borchert, S Mitchell, S Connelly
Reference-11
Exploring The Intersection of AI and Cybersecurity
M Maity
Reference-12
Unweaving the Cyber Attack-The Cyber Kill Chain Analysis
R Banerjee, D Mukherjee, PS Nayak, S Nath, MM Islam
Reference-13
Adversarial Examples in Machine Learning
I Goodfellow, J Shlens, C Szegedy