International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The Dangers of Public Wi-Fi: How to Protect Your Device Through Cyber Security

Dr. Rajan Gupta (Associate Professor) School of Information Technology

Vivekananda Institute of Professional Studies- Technical Campus, New Delhi
Prof. (Dr.) Supriya Madan (Professor) School of Information Technology
Vivekananda Institute of Professional Studies- Technical Campus, New Delhi
Dr. Indu Sahu (Assistant Professor) School of Information Technology
Vivekananda Institute of Professional Studies- Technical Campus, New Delhi
Raghav Goyal (Senior Software Engineer)
Gemini Solutions Pvt. Ltd., Gurugram, Haryana

Abstract: The public Wi-Fi networks become more and more common, there are numerous risks to personal cybersecurity. This article explores the hidden risks users encounter when connecting to these public networks, including malware distribution, surveillance, and attacks known as man in the middle. It also looks at doable standards for cybersecurity along with measures, like turning on firewalls and using virtual private networks (VPNs), that can help reduce these risks. There is an emphasis on the possible consequences of cybersecurity breaches, which can include anything from data theft to monetary losses. The article also looks at the statutory and regulatory structures that control the security of public Wi-Fi. Lastly, it points out gaps in the body of knowledge, opening the door for more studies and suggestions in this important area. This research looks at the potential dangers of utilising public Wi-Fi and offers workable cybersecurity recommendations for protecting mobile devices. The research is organised around three main topics such as security flaws in public Wi-Fi networks, the success of various cybersecurity methods, and the importance of educating and protecting end users. The first topic discusses how to spot and assess dangers like eavesdropping and man-in-the-middle attacks when using public Wi-Fi. The effectiveness and usefulness of VPNs and encryption techniques are evaluated in the second topic. The third principle stresses the value of advising users on how to keep their Wi-Fi connections safe and secure through consumer education. This research attempts to provide a thorough comprehension of device security in public Wi-Fi settings through thematic secondary data analysis. The results and suggestions are meant to provide consumers with the tools they need to safeguard their devices in advance, leading to a more secure time spent online.

Keywords: *Wi-Fi networks, Security Measure, VPN, CFAA*

I. INTRODUCTION

A. Project Specification

The scope and goals of the research project are described in the undertaking specification. It looks into the vulnerabilities that come with using public Wi-Fi networks as well as looks into cybersecurity solutions that can protect devices in those kinds of settings. The study aims to provide an in-depth comprehension of the weaknesses found in public Wi-Fi, examine possible risks, and determine whether different security methods are applicable. In order to achieve a thorough study, it is also used a structured method of investigation and critical review of the body of existing research. The principal objective of the research is to augment cognizance and expertise concerning public Wi-Fi encryption while providing useful perspectives for safeguarding devices.

B. Aim and Objectives

Aim

Investigating public Wi-Fi networks for weaknesses and investigating practical cybersecurity solutions to protect personal devices from potential threats are the goals of this research.

Objectives

- To identify and evaluate the several threats that free Wi-Fi access points pose to user privacy and the safety of devices.
- To assess the effectiveness of various cybersecurity techniques and instruments in reducing these threats.
- To acquire a thorough comprehension of the tenets, tactics, and industry best practices for guaranteeing personal device security when utilizing public Wi-Fi.
- To offer useful advice on how consumers can improve their understanding of cybersecurity and put precautions in place to keep their devices safe when using public Wi-Fi networks.

C. Research Rationale

The rationale underlying the research emphasizes how important it is to look into the dangers of using public Wi-Fi networks as well as why cybersecurity precautions are

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

necessary. The widespread use of free wireless internet and the possible risks it brings to users' gadgets and their private data are what spurred this investigation. In order to protect people from data interception, virus propagation, and other cyber threats, cybersecurity must address these risks. In order to fully realize the wider consequences of reducing these dangers and improving public Wi-Fi security thereby guaranteeing the safety of personal information and privacy it is imperative to comprehend the reasoning behind the current study.

II. LITERATURE REVIEW

A. Cybersecurity Threats in Public Wi-Fi Environments

A variety of dangers can jeopardize user safety and confidentiality when it comes to cybersecurity in free wireless environments. One common threat is eavesdropping, which is when uninvited parties intercept data that is transferred between machines and the network [1]. Passwords and private communications are among the sensitive data that could be obtained as a result of this hack. Another worry is man-in-the-middle (MitM) assaults.

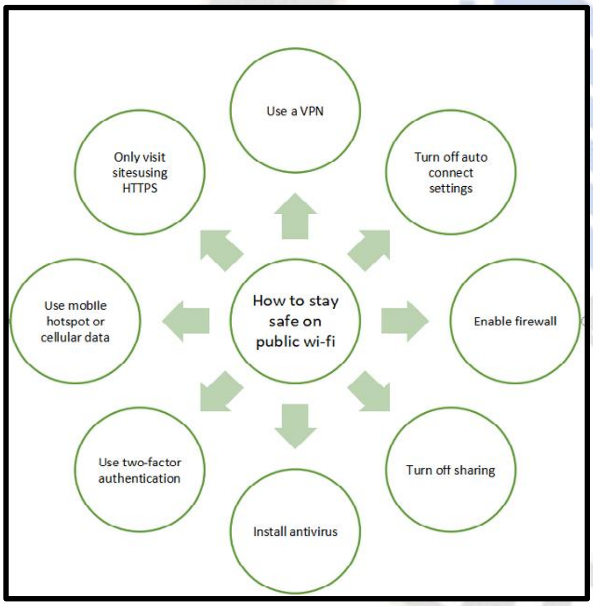
Use a VPN
Turn off auto connect settings
Enable firewall
Turn off sharing
Install antivirus
Use two-factor authentication
Use mobile hotspot or cellular data
Only visit sitesusing HTTPS
How to stay safe on public wi-fi

Fig. 2.1: Cybersecurity Threats in Public Wi-Fi Environments

By placing themselves in the way of users and the system as a whole, cybercriminals are able to intercept and alter data covertly. Such attacks lead to theft, data modification, or even the spread of malicious software [2]. Public wireless networks are frequently used as distribution channels for malware. Cybercriminals utilize open networks as a means of infecting users' devices with malware, which can result in data loss, machine compromise, and illegal access [3].

B. Cybersecurity Measures and Best Practices

To protect devices with confidential data, public Wi-Fi situations must implement security precautions and standards of excellence. A basic precaution is to use a Virtual Private Network (VPN), which encrypts transmissions of data to make them less susceptible to interception [4]. It is wise to steer clear of sensitive purchases on open networks to lower the chance of private and financial information being exposed.

Fig. 2.2: Cybersecurity Measures and Best Practices

The computer's defence against possible spyware threats that might be encountered in these types of shared environments is strengthened by turning on antivirus as well as firewall software. Selecting safe, password-protected connections and networks is a major step toward protection [5]. In order to avoid unintentionally connecting to rogue hotspots, it is crucial to confirm network names with employees. It is essential to update device software on a regular basis because updates frequently contain security patches that fix known vulnerabilities.

C. Impact and Consequences of Cybersecurity Breaches

Breach of security measures in public Wi-Fi networks can have negative, far-reaching effects. First of all, theft of identities and financial loss results because of the compromise of private and sensitive data, including financial data as well as passwords for accounts [6]. These violations also cause harm to one's reputation and erode public confidence in people, organizations, and enterprises.

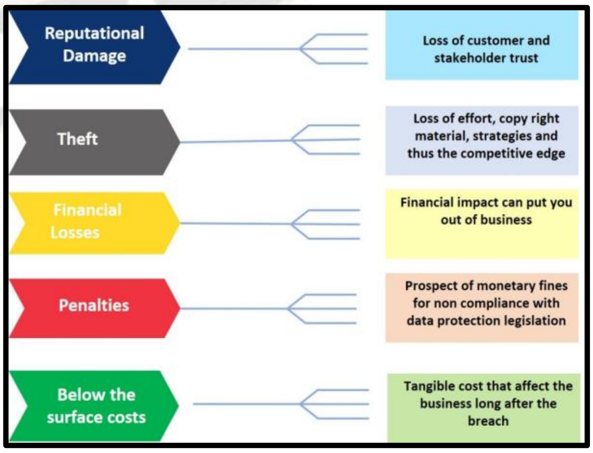
Reputational Damage
Loss of customer and stakeholder trust
Theft
Loss of effort, copy right material, strategies and thus the competitive edge
Financial Losses
Financial impact can put you out of business
Penalties
Prospect of monetary fines for non compliance with data protection legislation
Below the surface costs
Tangible cost that affect the business long after the breach

Fig. 2.3: Impact and Consequences of Cybersecurity Breaches

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Cybercriminals might also use these breaches as cover for additional attacks, which would compound the initial damage. Beyond just the losses that occur right away, there are legal fees, remediation costs, and possible regulatory penalties [7]. Cybersecurity lapses can also impair vital systems and services, resulting in decreased revenue and downtime. Cyberattacks on public Wi-Fi can have far-reaching effects on sensitive government data and vital infrastructure, raising issues with national security [8].

D. Legal and Regulatory Frameworks for Public Wi-Fi Security

The protection of users' information and anonymity in free wireless environments is contingent upon the existence of regulatory and legal systems. A number of nations have put in place particular laws and guidelines to deal with the problems related to public Wi-Fi security [9]. For example, the Act to Combat Computer Fraud and Abuse (CFAA) within the US is a crucial piece of legislation that deals with illegal access to computer equipment, including those linked to open wireless broadband networks [10].

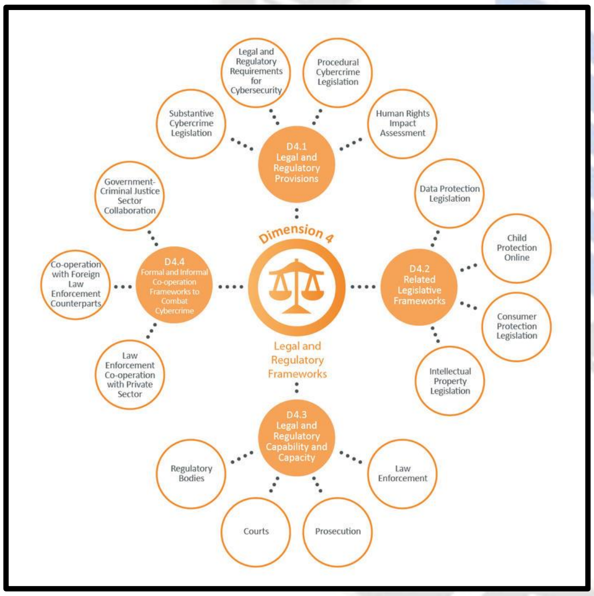
Legal and Regulatory Requirements for Cybersecurity
Procedural Cybercrime Legislation
Substantive Cybercrime Legislation
Human Rights Impact Assessment
D4.1 Legal and Regulatory Provisions
Government-Criminal Justice Sector Collaboration
Data Protection Legislation
Dimension 4
Child Protection Online
Co-operation with Foreign Law Enforcement Counterparts
D4.4 Formal and Informal Co-operation Frameworks to Combat Cybercrime
D4.2 Related Legislative Frameworks
Consumer Protection Legislation
Legal and Regulatory Frameworks
Law Enforcement Co-operation with Private Sector
Intellectual Property Legislation
D4.3 Legal and Regulatory Capability and Capacity
Regulatory Bodies
Law Enforcement
Courts
Prosecution

Fig. 2.4: Legal and Regulatory Frameworks for Public Wi-Fi Security

The Federal Trade Commission (FTC) is also able to take steps against organizations that do not sufficiently secure free Wi-Fi connections. Strict data protection regulations are enforced in the European Union under the General Data Protection Regulation (GDPR), even when using public Wi-Fi [11]. Organizations along with public Wi-Fi providers are required by GDPR to use encryption along with user consent to protect data confidentiality and safety [12]. Other countries have their own rules and guidelines that frequently deal with matters like user permission for collecting information, information retention, and breach notification.

E. Literature Gap

The majority of the literature that is currently available on wireless network security focuses on discovering dangers related to cybersecurity and suggesting countermeasures. On the other hand, research on the changing hazards and weaknesses in free Wi-Fi access points is conspicuously lacking. Research on emerging threats needs to be more thorough and current due to the speed at which technology along with cybercriminal tactics are developing. Furthermore, although regulatory and legal structures are covered to some extent, more research is needed to determine the efficacy of these strategies and how they affect public Wi-Fi protection. Future studies should investigate new threats and assess the effectiveness of legal and regulatory protections regarding public wireless network security in an effort to close these gaps.

III. METHODOLOGY

A. Research Philosophy

In this study, positivism has been used as the guiding research philosophy and this is selected for its empirical and scientific approach, measurement, emphasising objective observation and experimentation to develop trustworthy and valid information.

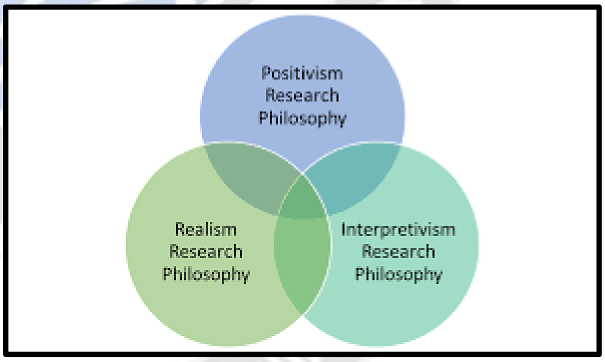
Positivism Research Philosophy
Realism Research Philosophy
Interpretivism Research Philosophy

Fig. 3.1: Types of research philosophy

Positivism provides a structured framework for rigorous data collecting, analysis, and assessment that is useful during the risk analysis of public Wi-Fi and the implementing of cybersecurity solutions [13]. This outlook is congruent with the project's goals and objectives, as it permits a thorough analysis of the dangers posed by free Wi-Fi access points and the evaluation of the efficacy of cybersecurity solutions [14]. The study is conducted using positivist methods in an effort to generate quantitative and repeatable findings that add to an understanding of how to keep private devices safe on public Wi-Fi networks.

B. Research Approach

This study uses a logical method of inquiry and the goal of deductive inquiry is to find evidence that supports a presupposed theory or hypothesis.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

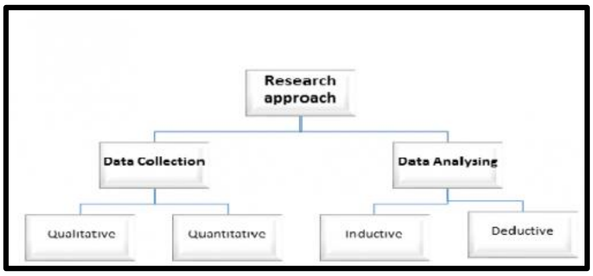

Fig. 3.2: Segment of research approach

A deductive method is suitable for this study on public Wi-Fi hazards and cybersecurity solutions because it permits a systematic review of existing theories and industry best practices surrounding device security in public Wi-Fi networks [15]. The study's overarching goal is to use collected data to confirm or improve upon previously established principles. This method provides a systematic and rational framework for dealing with the project's goals, guaranteeing a thorough analysis of potential risks and the efficacy of cybersecurity measures.

C. Research Design

A descriptive design has been used and the goal of descriptive design is to present a comprehensive and accurate picture of a phenomena or subject. Descriptive research designs are well-suited for the purposes of analysing public Wi-Fi risks and establishing cybersecurity remedies because they permit a thorough analysis of the numerous dangers and current practices without requiring the manipulation of variables [16]. This setup allows for extensive user behaviour, vulnerability and current cybersecurity measure data collection in public Wi-Fi settings for study [17]. The study takes a descriptive approach in an effort to provide a comprehensive understanding of the situation upon which to build knowledgeable suggestions for bolstering device security.

D. Data Analysis and Collection Method

Finding, examining and explaining overarching themes in preexisting qualitative data is what theorists call "thematic secondary data analysis." This method has been selected for the project on public Wi-Fi risks and cybersecurity because it permits a thorough investigation of users' experiences, behaviours, and attitudes in regard to device security [18]. Learners can learn more about the issues people have and the tactics they use to overcome them when using public Wi-Fi if they extract themes from the data that has already been gathered. Along with its goal of providing actionable advice on device security, this project also employed thematic analysis to gain a more nuanced knowledge of user viewpoints and practises [19]. Using secondary sources rather than conducting original research helps to save both time and money.

E. Ethical Consideration

The study has maintained all the rules and regulations of the government that help to implement the study without any hassle. The acquired information does not harm society and in that case, use public platforms not use any private platforms. The company Learners take precautions to minimise any possible physical, psychological, or social harm that participants can experience as a result of their engagement.

IV. RESULTS AND DISCUSSION

A. Critical Analysis

The topics cover the most important features of this research into the safety of public Wi-Fi. The first factor, "vulnerabilities," does a good job of highlighting the importance of knowing the nature of the threats in order to develop adequate defences [20]. While this research is useful as-is, it has been improved with a deeper dive into individual vulnerabilities. Important insights into the efficacy of security measures have been gained from the second theme that evaluates cybersecurity tactics. This has been improved by combining a broader range of methods and thinking about how they can work together [21]. The study focuses on educating consumers, an essential but often overlooked part of the cybersecurity puzzle. Case studies and real-world examples demonstrating how these safety measures might be put into practice are very helpful.

B. Theme 1: Issues identification with Public Wi-Fi Network Security

The focus is on pinpointing and assessing the numerous risks that open Wi-Fi networks represent to individual privacy and electronic security [22]. The process entails identifying security holes in public Wi-Fi networks that might be exploited by thieves.

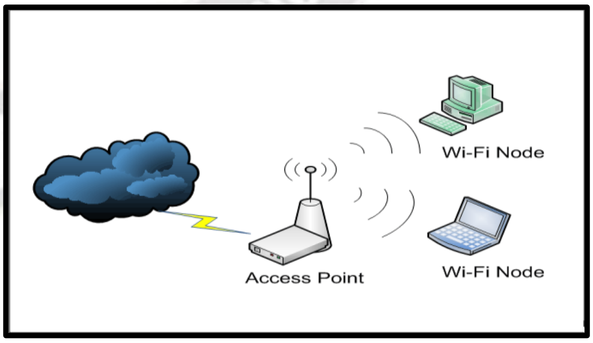

Fig. 4.1: Segment of research approach

Vulnerabilities include poor encryption, insecure networks and rogue access points. The development of reliable cybersecurity methods to safeguard individual devices relies on a firm grasp of these flaws [23]. The purpose of this research is to learn more about the unique dangers that come with using public Wi-Fi. Possible threats include eavesdropping on private conversations, man-in-the-middle assaults and data interception [24]. This study aims to shed light on the risks of using public Wi-Fi by investigating these vulnerabilities in depth.

C. Theme 2: Cybersecurity Techniques and Their Success

The goal of this section is to evaluate the effectiveness of various cybersecurity methods and tools in a comprehensive way [25]. Examining the usefulness and effect of various security solutions including VPNs, firewalls, encryption technologies, and authentication techniques [26]. The objective is to find out how best to protect one's own devices when connected to a public Wi-Fi network.

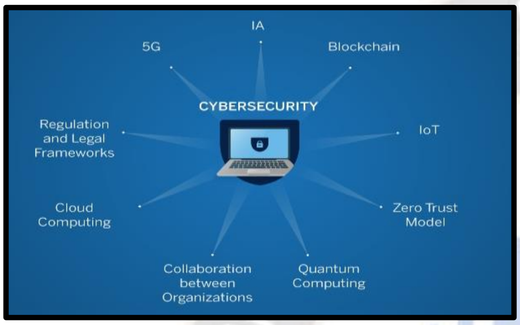

Fig. 4.2: Security factors

The purpose of the study is to do such evaluations of cybersecurity practices and technologies. Scientists also examine collected information to see how well these methods mitigate the noted dangers [27]. They may, for instance, gauge the level of encryption provided by a “virtual private network (VPN)” or assess the efficacy of intrusion detection and prevention software. This topic sheds light on the real-world implications of certain cybersecurity precautions.

D. Theme 3: Warn and Educate Shoppers

Using public Wi-Fi networks safely requires knowledge and awareness on the part of customers and this subject highlights the significance of educating consumers on cybersecurity. It entails advising users on steps they take to better secure their systems and educate themselves on cybersecurity issues [28]. Users' knowledge and actions are acknowledged as critical to protecting their devices. The study overarching goal is to offer customers useful recommendations within this context. Advice on selecting safe networks, creating and using strong passwords, and maintaining current versions of programs and apps has been provided. The study also focused on how to spot typical social engineering strategies employed by cybercriminals [29]. The study intends to equip people to proactively secure their devices when using public Wi-Fi by concentrating on consumer education and precautions.

E. Discussion

These three themes help illuminate the risks of using public Wi-Fi and the importance of employing cybersecurity safeguards to secure one's own devices. In order to improve device security in public Wi-Fi situations, the project intends to address vulnerabilities, evaluate the efficacy of security methods and promote consumer education. The research topics on public Wi-Fi security show a comprehensive strategy since they encompass both technical and pedagogical aspects of the problem [30]. This guarantees a comprehensive study of safeguarding devices in open Wi-Fi networks. Individuals and businesses benefit from the study's findings since they deconstruct weaknesses and evaluate the efficiency of cybersecurity solutions. Moreover, the emphasis on consumer education and measures emphasises the crucial role of user awareness in increasing device security. This all-encompassing strategy is consistent with the study's primary purpose of providing actionable suggestions for protecting individual devices when using shared Wi-Fi hotspots.

V. CONCLUSION

A. Critical Evaluation

A critical assessment of the literature demonstrates the widespread vulnerabilities connected to public Wi-Fi networks, including malware distribution, eavesdropping, and attacks via man in the middle. The necessity of cybersecurity measures to reduce the risks is highlighted by these threats. Although recommended practices are sufficiently outlined by existing research, constant vigilance along with adaptability are necessary due to the dynamic nature of digital dangers. The potential consequences of security breaches, such as harm to one's finances and reputation, also serve to highlight how important these preventative measures are. Furthermore, even though they are crucial, the regulatory and legal systems might need to be further developed and harmonized. The body of research emphasizes how urgent it is to strengthen Wi-Fi access in public places security in order to adequately protect online transactions.

B. Research Recommendation

More research is highly advised in view of the current dangers to cybersecurity and the constantly changing public Wi-Fi protection landscape format. Researchers ought to concentrate on developing cutting-edge security protocols that are and tools as well as investigating new hazards and weaknesses in public Wi-Fi surroundings. Furthermore, analyzing user behaviors as well as awareness regarding the adoption of security protocols on free Wi-Fi access points yield insightful information. Collaborations between academic institutions, businesses, and governmental organizations ought to be promoted in order to deepen understanding of these problems and help create all-encompassing plans for protecting users from free Wi-Fi. In that setting, research projects of this kind can be essential to tackling the constantly changing makeup of dangers to cybersecurity.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

C. Future Work

The goal of future research in the area of public WiFi safety should be to continuously adjust to new threats to the network. Particularly for those with no technical expertise, researchers should look into creating cybersecurity tools that are more reliable and easy to use. Furthermore, it is crucial to continuously monitor and analyze regulatory changes and how they affect the security of public Wi-Fi. An area of research that shows promise is examining the ways in which the “Internet of Things (IoT)” interacts with free wireless networks and any possible holes in it. Government, business, and academic cooperation are essential to preventing cyberattacks and guaranteeing the long-term safety of public wireless networks.

VI. REFERENCES

[1] I. O. Ogundele *et al*, "A Review of Smartphone Security Challenges and Prevention," *International Research Journal of Innovations in Engineering and Technology,* vol. 7, *(5),* pp. 234-245, 2023. Available: https://www.proquest.com/scholarly-journals/review-smartphone-security-challenges-prevention/docview/2833995412/se-2. DOI: https://doi.org/10.47001/IRJIET/2023.705030.

[2] C. Gupta *et al*, "A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks," *Sensors,* vol. 22, *(5),* pp. 2017, 2022. Available: https://www.proquest.com/scholarly-journals/systematic-review-on-machine-learning-deep-models/docview/2637816482/se-2. DOI: https://doi.org/10.3390/s22052017.

[3] I. Makhdoom, "Defense Against Integrity and Privacy Attacks in the Internet of Things." Order No. 30611709, University of Technology Sydney (Australia), Australia, 2020.

[4] S. N. Ashraf *et al*, "IoT empowered smart cybersecurity framework for intrusion detection in internet of drones," *Scientific Reports (Nature Publisher Group),* vol. 13, *(1),* pp. 18422, 2023. Available: https://www.proquest.com/scholarly-journals/iot-empowered-smart-cybersecurity-framework/docview/2882802221/se-2. DOI: https://doi.org/10.1038/s41598-023-45065-8.

[5] C. E. Bamborough, "The Architect’s Measure: Constructing a Character and Influence for Data in Practice." Order No. 30668352, University of Technology Sydney (Australia), Australia, 2023.

[6] M. M. Aslam *et al*, "A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects," *Sensors,* vol. 23, *(18),* pp. 7999, 2023. Available: https://www.proquest.com/scholarly-journals/comprehensive-study-on-cyber-attacks/docview/2869625031/se-2. DOI: https://doi.org/10.3390/s23187999.

[7] I. Seth *et al*, "A Taxonomy and Analysis on Internet of Vehicles: Architectures, Protocols, and Challenges," *Wireless Communications & Mobile Computing (Online),* vol. 2022, 2022. Available: https://www.proquest.com/scholarly-journals/taxonomy-analysis-on-internet-vehicles/docview/2675430859/se-2. DOI: https://doi.org/10.1155/2022/9232784.

[8] F. N. Turner, "From Chaos to Calm: A Narrative Multiple Case Study Investigating Crisis Experiences of K–12 Executive Leaders of Curriculum and Instruction." Order No. 28970622, Baylor University, United States -- Texas, 2022.

[9] D. M. Berry, "The Explainability Turn," *Digital Humanities Quarterly,* vol. 17, *(2),* 2023. Available: https://www.proquest.com/scholarly-journals/explainability-turn/docview/2842907219/se-2.

[10] Z. Muhammad *et al*, "Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses," *Technologies,* vol. 11, *(3),* pp. 76, 2023. Available: https://www.proquest.com/scholarly-journals/smartphone-security-privacy-survey-on-apts-sensor/docview/2829870441/se-2. DOI: https://doi.org/10.3390/technologies11030076.

[11] O. A. Abasi-amefon *et al*, "IoT Health Devices: Exploring Security Risks in the Connected Landscape," *IoT,* vol. 4, *(2),* pp. 150, 2023. Available: https://www.proquest.com/scholarly-journals/iot-health-devices-exploring-security-risks/docview/2829811948/se-2. DOI: https://doi.org/10.3390/iot4020009.

[12] M. M. Alani and E. Damiani, "XRecon: An Explainbale IoT Reconnaissance Attack Detection System Based on Ensemble Learning," *Sensors,* vol. 23, *(11),* pp. 5298, 2023. Available: https://www.proquest.com/scholarly-journals/xrecon-explainbale-iot-reconnaissance-attack/docview/2824015466/se-2. DOI: https://doi.org/10.3390/s23115298.

[13] A. Falayi *et al*, "Survey of Distributed and Decentralized IoT Securities: Approaches Using Deep Learning and Blockchain Technology," *Future Internet,* vol. 15, *(5),* pp. 178, 2023. Available: https://www.proquest.com/scholarly-journals/survey-distributed-decentralized-iot-securities/docview/2819445882/se-2. DOI: https://doi.org/10.3390/fi15050178.

[14] U. Tariq *et al*, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors,* vol. 23, *(8),* pp. 4117, 2023. Available: https://www.proquest.com/scholarly-journals/critical-cybersecurity-analysis-future-research/docview/2806590738/se-2. DOI: https://doi.org/10.3390/s23084117.

[15] D. Oladimeji *et al*, "Smart Transportation: An Overview of Technologies and Applications," *Sensors,* vol. 23, *(8),* pp. 3880, 2023. Available: https://www.proquest.com/scholarly-journals/smart-transportation-overview-technologies/docview/2806590557/se-2. DOI: https://doi.org/10.3390/s23083880.

[16] M. Murrell, "Ethics in a Technical World," *GPSolo,* vol. 40, *(1),* pp. 20-24, 2023. Available: https://www.proquest.com/trade-journals/ethics-technical-world/docview/2778660234/se-2.

[17] Z. Muhammad *et al*, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," *Energies,* vol. 16, *(3),* pp. 1113, 2023. Available: https://www.proquest.com/scholarly-journals/emerging-cybersecurity-privacy-threats-electric/docview/2774895559/se-2. DOI: https://doi.org/10.3390/en16031113.

[18] Anonymous "Automotive markets intelligence service: 2023 Q1 edition: Industry megatrends," GlobalData plc, London,

2023Available: https://www.proquest.com/reports/automotive-markets-intelligence-service-2023-q1/docview/2766668063/se-2.

[19] A. S. Toqeer *et al*, "In-Depth Review of Augmented Reality: Tracking Technologies, Development Tools, AR Displays, Collaborative AR, and Security Concerns," *Sensors*, vol. 23, *(1)*, pp. 146, 2023. Available: https://www.proquest.com/scholarly-journals/depth-review-augmented-reality-tracking/docview/2761206929/se-2. DOI: https://doi.org/10.3390/s23010146.

[20] A. Clim *et al*, "The Need for Cybersecurity in Industrial Revolution and Smart Cities," *Sensors*, vol. 23, *(1)*, pp. 120, 2023. Available: https://www.proquest.com/scholarly-journals/need-cybersecurity-industrial-revolution-smart/docview/2761205658/se-2. DOI: https://doi.org/10.3390/s23010120.

[21] H. H. A. Theyazn and H. Alkahtani, "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model," *Mathematics*, vol. 11, *(1)*, pp. 233, 2023. Available: https://www.proquest.com/scholarly-journals/cyber-security-detecting-distributed-denial-xa0/docview/2761189090/se-2. DOI: https://doi.org/10.3390/math11010233.

[22] M. Lei *et al*, "Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges," *Foods*, vol. 11, *(15)*, pp. 2262, 2022. Available: https://www.proquest.com/scholarly-journals/integration-privacy-protection-blockchain-based/docview/2700564780/se-2. DOI: https://doi.org/10.3390/foods11152262.

[23] Y. Xu, S. Liu and Y. Chen, "On the Problems and Countermeasures of College Students' Mental Health and Safe Work under Network Environment," *Journal of Environmental and Public Health*, vol. 2022, 2022. Available: https://www.proquest.com/scholarly-journals/on-problems-countermeasures-college-students/docview/2701962723/se-2. DOI: https://doi.org/10.1155/2022/2993982.

[24] T. Mo *et al*, "Trends and Emerging Technologies for the Development of Electric Vehicles," *Energies*, vol. 15, *(17)*, pp. 6271, 2022. Available: https://www.proquest.com/scholarly-journals/trends-emerging-technologies-development-electric/docview/2711324345/se-2. DOI: https://doi.org/10.3390/en15176271.

[25] A. Tăbușcă, G. Garais and A. Enăceanu, "CYBERSECURITY EDUCATION – THE NEW LITERACY," *Journal of Information Systems & Operations Management*, vol. 16, *(2)*, pp. 263-272, 2022. Available: https://www.proquest.com/scholarly-journals/cybersecurity-education-new-literacy/docview/2771102439/se-2.

[26] T. Sutikno and D. Thalmann, "Insights on the internet of things: past, present, and future directions," *TELKOMNIKA*, vol. 20, *(6)*, pp. 1399-1420, 2022. Available: https://www.proquest.com/scholarly-journals/insights-on-internet-things-past-present-future/docview/2724915342/se-2. DOI: https://doi.org/10.12928/TELKOMNIKA.v20i6.22028.

[27] K. A. Alaghbari *et al*, "Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations," *Journal of Cloud Computing*, vol. 11, *(1)*, 2022. Available: https://www.proquest.com/scholarly-journals/complex-event-processing-physical-cyber-security/docview/2724782633/se-2. DOI: https://doi.org/10.1186/s13677-022-00338-x.

[28] H. S. Choi, D. Carpenter and M. S. Ko, "Risk Taking Behaviors Using Public Wi-Fi™," *Inf. Syst. Front.*, vol. 24, *(3)*, pp. 965-982, 2022. Available: https://www.proquest.com/scholarly-journals/risk-taking-behaviors-using-public-wi-fi™/docview/2705908370/se-2. DOI: https://doi.org/10.1007/s10796-021-10119-7.

[29] Z. Wang *et al*, "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," *Sustainability*, vol. 14, *(19)*, pp. 12409, 2022. Available: https://www.proquest.com/scholarly-journals/security-issues-solutions-connected-autonomous/docview/2724321218/se-2. DOI: https://doi.org/10.3390/su141912409.

[30] M. N. Reid, "Optical Wireless Communications High-Speed Bluetooth Secure Pairing Towards Developing a Trust Protocol." Order No. 30246444, Pace University, United States -- New York, 2022.