REVIEW ON DYNAMICS OF CYBER CRIMES AND AWARENESS: A STUDY IN BIHAR

Ajit Kumar[1], Om Prakash Roy[2]
E-Mail Id: ajitjnvassam@gmail.com
[1]Research Scholar, University Department of Mathematics, B. R. A. Bihar University, Muzaffarpur, Bihar, India
[2]Professor, Department of Physics, B.R.A. Bihar University, Muzaffarpur, Bihar, India
[2]L. S. College, Muzaffarpur, Bihar, India

Abstract- The research examines the dynamics of cybercrimes and awareness in Bihar, focusing on the changing environment of cyber threats in the region. It also investigates approaches to improve cyber security awareness and implement steps to mitigate these threats. This study does a thorough analysis to investigate the prevalence, various types, and consequences of cybercrimes on both persons and organizations in the state of Bihar. This study examines the primary determinants that contribute to the escalation of cybercrimes, encompassing developments in technology, heightened internet connectivity, and insufficient cyber security protocols. This study highlights the pressing necessity for increased consciousness and proactive strategies to successfully mitigate cyber dangers. An alarming rise of cybercrimes targeting citizens and businesses in Bihar, including financial scams, identity theft, cyber bullying, and data breaches, is one of the main conclusions of the study. These criminal activities not only lead to substantial monetary damages but also erode confidence, jeopardize confidentiality, and jeopardize the digital welfare of persons and communities. The research emphasizes the need of advocating for cyber security awareness campaigns and equipping individuals with information regarding cyber dangers and optimal strategies for ensuring online safety. The research underscores the importance of fostering collaborative endeavors among governmental entities, law enforcement agencies, educational establishments, and industry participants in order to effectively address cyber threats in a holistic manner. Stakeholders can bolster cyber resilience at both the human and organizational levels by cultivating collaborations, exchanging resources, and synchronizing response endeavors. The research closes by providing suggestions for improving cyber security awareness and adopting effective mitigation techniques to protect against cyber threats in Bihar and other regions.

Keywords: Cybercrimes, Awareness, Mitigation, Bihar, Cyber security, Threats, Prevention, Education, Collaboration, Resilience.

1. INTRODUCTION

The complex realm of cybercrimes and awareness in Bihar has various dimensions that intersect with technology, society, and governance. Being one of the largest states in India, Bihar encounters distinctive obstacles in addressing cybercrimes while concurrently fostering awareness among its population. This study aims to analyse the complexities involved, providing insights into the changing nature of cyber risks and the growing importance of increased awareness in the state of Bihar. The state of Bihar, renowned for its extensive cultural legacy, is currently undergoing a swift shift towards a digital age, marked by heightened internet accessibility and improvements in technology. Although these advancements present a multitude of prospects for expansion and interconnectedness, they also provide individuals, corporations, and government agencies with exposure to diverse cyber risks. The realm of cybercrimes encompasses a wide range of activities, including phishing schemes, identity theft, and virus attacks, which are always changing and expanding. Gaining insight into the trends and patterns of cybercrimes in Bihar is of paramount importance in formulating efficacious mitigation methods[1], [2]. The examination demonstrates a notable increase in cyber assaults that specifically aim at financial institutions, government entities, and naïve individuals. The rapid increase in the number of mobile devices and social media platforms has made it easier for disinformation and cyber bullying to propagate, making the situation worse. Multiple variables contribute to the high incidence of cybercrimes in Bihar. Prominent issues arise from socio-economic inequality, restricted digital literacy, and insufficient cybersecurity infrastructure.

Fig. 1.1 Dynamics of cybercrimes[3]

The expeditious rate at which technology improvements occur frequently surpasses the capacity of regulatory frameworks and law enforcement capacities, so generating vulnerabilities that cyber criminals exploit for their own benefit. Cyber-crimes have a wide-ranging impact that goes beyond only financial losses. Victims frequently experience psychological distress, reputational harm, and a decline in trust towards internet networks. Cyber-attacks can cause operational disruptions, loss of valuable information, and damage to brand image for enterprises. Cyber threats in the domain of governance provide a significant risk to the security of a nation, hence requiring the implementation of strong and effective cyber defense systems. The cultivation of awareness plays a crucial role in enabling individuals and organizations to effectively safeguard themselves against cyber threats. The inclusion of initiatives focused on improving digital literacy, advocating for secure online behaviors, and cultivating a cyber-security-oriented environment are integral elements of this undertaking[4]–[6]. The effective dissemination of information and resources necessitates the incorporation of collaborative endeavors among government agencies, educational institutions, and industry stakeholders. It is imperative that mitigation efforts adopt a comprehensive strategy that incorporates technology solutions, legislative reforms, and capacity-building initiatives. Enhancing cyber security infrastructure, implementing training initiatives for law enforcement professionals, and establishing dedicated cyber-crime investigative teams are critical measures in advancing this objective. Furthermore, public-private collaborations have the potential to enhance the exchange of knowledge and foster collaboration in the fight against cyber-crimes. To summarize, the interplay between cybercrimes and awareness in Bihar is a multifaceted system that necessitates collaborative attempts from all parties involved. To enhance its resilience against cyber risks, Bihar should comprehend the dynamic characteristics of cyber dangers, tackle the fundamental socio-economic causes, and give priority to raising awareness and implementing mitigation techniques.

2. RELATED WORK

Navitha 2023 et al. to examine instances of cybercrimes targeting women and children in India spanning the years 2017 to 2021. The analysis will rely on secondary data obtained from the National Crime Records Bureau website. The findings suggest an upward trajectory in cybercrimes on a yearly basis. Women are frequently subjected to internet pornography, cyber stalking, and cyber bullying, whilst children are frequently targeted by cyber pornography, cyber blackmailing, and online stalking. The annual increase in the proportion of cybercrimes targeting women and children, as well as the overall increase in cybercrimes and crimes against women and children, is evident. Typically, women are the target of 20.272% of cybercrimes in India, while 2.048% of crimes against women are classified as cybercrimes. Similarly, children are the target of 1.346% of cybercrimes, while cybercrimes account for 0.446% of crimes against children[7]

Song 2022 et al. Amidst a period of increasing technological intricacy, the importance of cybersecurity and privacy is of utmost significance. This study focuses on the urgent requirement to protect the digital identities and ensure the safety of preschool-aged children online. This paper presents a novel cybersecurity management system for preschools, which is powered by intelligent agents. This study seeks to enhance the resilience of preschools against contemporary threats by employing innovative methodologies. The objective is to facilitate prompt reactions to cyber incidents, while simultaneously ensuring the protection of essential systems and personal data. Through the integration of dispersed systems and the resolution of intricate issues, this novel approach possesses the capacity to substantially enhance cybersecurity standards in the realm of early education. It presents a pragmatic framework for guaranteeing digital security for young learners[8].

Patil 2022 et al. The increase in digitization has resulted in a corresponding increase in cybercrimes, which presents difficulties in forensic investigations as a result of insufficient network protocols for gathering evidence. The current methods only extend to the Internet Service Provider (ISP) and lack primary proof. The approach we propose aims to enhance the process of tracing to the genuine source by proactively collecting forensically good evidence. By employing an agent method, it gathers device data as a unique identifier, facilitating the process of non-repudiation. This fingerprinting technique utilizes a hash tree to produce unchangeable evidence that has been verified for legal purposes. The reliability of security validation is enhanced with the utilization of BAN logic and formal verification using the AVISPA tool. The implementation is supported by a prototype hosted on Amazon Web Services (AWS)[9].

Yogesh 2020 et al. Network forensic tools are crucial for collecting legal evidence of cybercrimes by capturing and analyzing network packets to track security breaches back to their origin. Nevertheless, current IP trace back methods frequently conclude inquiries at the edge router or ISP, so failing to ascertain the first assailant. Root-tracker is a safe system that utilizes device fingerprinting to locate cybercrime sources beyond the Internet Service Provider (ISP). Root-tracker, a prototype deployed on AWS, is designed to withstand attacker attempts to delete evidence. It continues to generate partial evidence match reports even after system modifications. Real-time testing confirms its effectiveness in tracking cybercriminals beyond the bounds of Internet Service Providers (ISPs), guaranteeing the integrity of forensic evidence in court procedures[10].

TABLE-2.1 LITERATURE SUMMARY

Author/year	Method/model	Research gap	Parameters	References
Alatawi/2023	Hybrid PSO-GA	Cybersecurity lacks	Cybersecurity demands	[11]

	model enhances cybersecurity with 100% accuracy.	effective intrusion detection despite advancing techniques.	enhanced intrusion detection amidst increasing cyber threats.	
Sumartiningsih/ 2023	Legal framework for personal data protection against hacking threats.	Legal enforcement inadequacies in personal data protection from hacking.	Personal data protection, legal basis, public awareness, hacking consequences.	[12]
Okutan/2022	Examining judicial process for combating information technology crimes comprehensively.	Gap in understanding cybercrime's impact and judicial system's efficacy.	Technological development, cybercrime types, judicial system evaluation, crime detection.	[13]
Tyunin/2021	Analyzing trends in cybercrimes against property using various methods.	Emerging trends in cybercrimes against property during pandemics.	Trends in criminalization of cybercrimes against property during pandemics.	[14]
Pawar/2021	Understanding and combating cybercrime in the digital realm.	Understanding cyber threats and enhancing cybersecurity measures effectively.	Understanding cyberspace dynamics and enhancing cybersecurity for data protection.	[15]

3. FACTORS CONTRIBUTING TO CYBER CRIMES

Cybercrimes pose a substantial and dynamic menace in our progressively digitised society, propelled by a myriad of interrelated elements. It is vital to comprehend these characteristics in order to build efficacious ways for countering cybercriminal activity. To begin with, the proliferation of cybercrimes is significantly influenced by technical improvements. The swift rate of technical advancement has resulted in the development of more intricate digital systems, presenting cybercriminals with a wide range of possibilities to take advantage of weaknesses. Cybercriminals utilise advanced technology to penetrate networks, pilfer confidential data, and carry out fraudulent activities, ranging from sophisticated virus attacks to complex phishing scams. The cybercrime scenario is worsened by global connection. Cybercriminals can exploit the interconnectedness of the internet to carry out their activities on a worldwide level, specifically targeting individuals, corporations, and governments regardless of their physical location. The extensive global presence of cybercriminals poses a significant obstacle for law enforcement authorities in effectively locating and prosecuting them. This is due to their ability to elude discovery by operating in governments with lenient cybersecurity rules[16]. The provision of anonymity and pseudonymity inside the digital domain constitutes an additional noteworthy element that contributes to the occurrence of cybercrimes. Cybercriminals possess the ability to obscure their identities by employing counterfeit email addresses, usernames, and IP addresses, hence posing challenges for law enforcement agencies in their efforts to identify and apprehend them. The presence of anonymity empowers cybercriminals to partake in unlawful acts without facing consequences, as they are aware that they are protected from being held accountable. The proliferation of cybercrimes is also propelled by economic incentives. Cybercriminals are driven to target individuals and organizations for monetary rewards due to the opportunity for financial gain. Cybercriminals exploit digital channels to illicitly profit by stealing credit card information, performing ransomware attacks, or participating in cryptocurrency fraud. This poses huge financial threats to victims and the greater economy[17], [18]. The absence of sufficient cybersecurity awareness among both individuals and organizations provides a conducive environment for the proliferation of cybercriminal incidents. A significant number of users are susceptible to prevalent strategies like phishing scams or downloading malware-infected files as a result of their limited comprehension of cybersecurity best practices. Likewise, organizations may fail to adopt strong cybersecurity protocols, so exposing themselves to cyberattacks that can lead to significant monetary losses and harm to their brand. The frequency of cybercrimes is further exacerbated by vulnerabilities present in digital infrastructure and systems. The presence of obsolete software, improperly designed systems, and insufficient security measures gives rise to vulnerabilities that can be exploited by cybercriminals in order to illicitly obtain access to confidential data. Furthermore, the widespread adoption of Internet of Things (IoT) devices has resulted in an increased vulnerability, hence presenting cybercriminals with novel avenues to infiltrate networks. The insufficiency of legislative frameworks pertaining to cybercrimes presents substantial obstacles to the endeavors of law enforcement[19], [20]. The laws and regulations pertaining to cybercrimes exhibit significant variation across different jurisdictions and May not consistently align with the rapid progress of technology. Consequently, law enforcement organizations encounter challenges in efficiently investigating and prosecuting cybercriminals, underscoring the necessity for enhanced and standardized legal frameworks at both domestic and global scales. The development of cybercrimes can be attributed to a confluence of factors including technological

advancements, global connectivity, anonymity, economic incentives, cybersecurity awareness, vulnerabilities in infrastructure, and insufficient regulatory frameworks. To effectively combat cybercrimes in the digital era, it is necessary for governments, law enforcement agencies, businesses, and individuals to collaborate and improve cybersecurity measures, increase awareness, and reinforce legal frameworks.

4. IMPACT AND CONSEQUENCES OF CYBER CRIMES

Cybercrimes, driven by swift technological progress and the growing interconnectivity of the digital sphere, have significant ramifications and effects that go well beyond the domain of digital security. Cybercrimes present substantial issues to individuals, corporations, governments, and communities at large, encompassing financial losses, national security risks, and individual privacy concerns.

4.1 Financial Losses and Economic Disruption

Cybercrimes have a direct and measurable effect on victims, primarily in the form of financial damages. The losses are a result of diverse types of cyberattacks, encompassing ransomware, phishing schemes, identity theft, and breach of business email. Businesses can experience substantial financial losses, disruptions in operations, harm to their brand, and legal obligations as a result of cybercrimes. According to a survey published by Cybersecurity Ventures, it is anticipated that the annual damages resulting from worldwide cybercrime would exceed $6 trillion by the year 2021. Furthermore, cybercrimes possess wider economic ramifications[21]–[23]. Digital technologies have the potential to erode customer confidence in online transactions, impede investment in such technologies, and cause disruptions in supply chains and vital infrastructure. Small and medium-sized organizations (SMEs) are susceptible to advanced cyber-attacks due to their limited resources and expertise in safeguarding against such threats.

4.2 Threats to National Security and Public Safety

Cybercriminal activities provide significant risks to both national security and public safety, especially when they are directed towards key infrastructure, government entities, and vital services. State-commissioned cyber espionage, cyberterrorism, and cyber warfare operations have the potential to jeopardize confidential government data, disrupt vital infrastructure like power grids and transportation networks, and weaken diplomatic connections between countries. Targeting healthcare facilities, emergency services, and law enforcement agencies with cybercrimes poses a significant threat to lives and undermines public safety. For instance, a cyber assault on a hospital's network has the potential to interrupt patient treatment, compromise medical records, and perhaps endanger patient safety.

4.3 Erosion of Privacy and Trust

Cybercrimes play a crucial role in undermining privacy rights and eroding trust in digital platforms and organizations. Exposing individuals to various sorts of exploitation, such as identity theft and financial fraud, occurs when their personal information is compromised through data breaches, cyber assaults, and unauthorized surveillance activities. The growing ubiquity of surveillance technologies and governmental surveillance initiatives raises concerns regarding the safeguarding of civil liberties and individual rights[24]–[26]. A decrease in trust towards digital platforms and institutions can have far-reaching implications for several facets of society. User engagement and adoption rates have experienced a decrease as a result of the erosion of trust in e-commerce, online banking, social networking, and digital services. Furthermore, this phenomena poses a threat to the core tenets of democratic societies as it erodes public trust in democratic processes, diminishes the credibility of the media, and hampers governmental transparency.

4.4 Societal Impacts and Cybersecurity Awareness

Cybercrimes possess wider societal ramifications, intensifying social disparities, cultivating skepticism, and maintaining disparities in digital access. Vulnerable populations, including persons with low income, minority groups, and the elderly, experience a disproportionate impact from cybercrimes as a result of their restricted access to cybersecurity tools and lack proficiency in digital literacy. Furthermore, cybercrimes have a significant role in exacerbating social differences, disseminating misinformation, and facilitating disinformation efforts, so eroding social cohesiveness and democratic principles. The mitigation and repercussions of cybercrimes necessitate a comprehensive strategy that entails cooperation among governmental bodies, enterprises, non-governmental organizations, and global institutions[27]. This encompasses the allocation of resources towards the development of cybersecurity infrastructure, the augmentation of cybersecurity education and awareness initiatives, the reinforcement of regulatory frameworks, and the promotion of international collaboration in order to successfully address cyber threats.

5. BUILDING AWARENESS AND MITIGATION STRATEGIES

The establishment of awareness and the implementation of efficient mitigation techniques are of utmost importance in addressing the increasing menace of cybercrimes. In the contemporary era of interconnected digital environments, characterized by the constant evolution of cyber dangers, it is imperative to adopt proactive measures in order to safeguard both individuals and organizations against potential harm. The initial step in

increasing awareness is providing education to individuals and corporations regarding the prevailing cyber hazards and the potential ramifications they may entail. One aspect of this involves acquainting individuals with prevalent methods of attack, such as phishing, malware, ransomware, and social engineering strategies. Training programmers ought to priorities the significance of identifying dubious activity, implementing effective cyber hygiene measures, and following to established security protocols. The prioritization of cybersecurity education and training for employees is crucial for organizations[28], [29]. To foster a culture of security awareness, it is beneficial to implement regular training, seminars, and simulated phishing exercises. It is imperative to provide employees with training in order to effectively recognize and swiftly report any risks, hence enhancing the organization's overall security stance. Ensuring the adoption of effective cyber hygiene procedures is crucial for reducing cyber risks. This entails promoting the adoption of robust and distinctive passwords, activating two-factor authentication, and ensuring the regular updating of software and systems. Regular security audits and assessments play a crucial role in the identification and timely resolution of vulnerabilities. Enforcing strong technical measures is crucial for ensuring efficient cybersecurity. In order to safeguard against unauthorized access and malicious activity, it is imperative for organizations to implement firewalls, intrusion detection systems, and antivirus software. The utilization of encryption methods is vital for the protection of sensitive data, both when stored and during transmission. The development and continuous testing of incident response strategies are crucial for the efficient management of cyber threats. The aforementioned plans delineate the sequential actions to be undertaken in the occurrence of a security breach, encompassing containment, eradication, and recovery protocols[30], [31]. Engaging in routine table top exercises and simulated cyber-attack scenarios can contribute to the organization's readiness in efficiently addressing crises. In summary, the establishment of awareness and the implementation of mitigation methods are fundamental components of a robust cybersecurity framework. Organisations can strengthen their resilience against cyber threats and mitigate possible damage by implementing strategies such as training individuals, supporting good cyber hygiene practices, deploying robust technical controls, and developing incident response plans.

CONCLUSION

In summary, the research conducted on the dynamics of cybercrimes and awareness in Bihar has yielded significant findings regarding the prevailing cyber risks in the area and the urgent requirement for increased knowledge and preventive measures. The varied nature of cybercrimes and their adverse impact on individuals, corporations, and society as a whole have been found through a detailed analysis. The study's results highlight the concerning increase in cybercrimes that specifically target individuals and institutions in Bihar. These crimes encompass a wide range of offences, including financial fraud, identity theft, cyberbullying, and data breaches. In addition to causing significant financial losses, these criminal activities also have detrimental effects on trust, privacy, and the overall digital well-being of individuals and communities[32]–[34]. The research emphasizes the crucial significance of awareness and education in the reduction of cyber risks and the cultivation of a cyber resilience culture. Through the implementation of cybersecurity awareness programmers, the dissemination of knowledge regarding cyber dangers to individuals, and the cultivation of best practices for online safety, it is possible to augment the level of preparation among the population of Bihar in effectively battling cybercrimes. The report also highlights the significance of fostering collaboration among government agencies, law enforcement authorities, educational institutions, and industry players in order to effectively tackle cyber risks in a holistic manner. Through the cultivation of alliances, the exchange of resources, and the synchronization of response endeavors, we can augment cyber resilience at both the individual and organizational tiers. To summarize, effectively dealing with the intricacies of cybercrimes and increasing public knowledge in Bihar requires a collaborative and coordinated endeavor from all parties involved. Through the strategic emphasis on cybersecurity education, the implementation of proactive measures, and the cultivation of collaborative efforts, it is possible to collaboratively mitigate cyber threats and establish a more secure digital environment for the inhabitants of Bihar[3], [35].

REFERENCES

[1] R. Kant, “Cyber-Security Awareness in India : How Much Students of Higher Cyber-Security Awareness in India: How Much Students of Higher Education Are Aware ?,” no. June, 2023.

[2] A. Johri and S. Kumar, “Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation,” Hum. Behav. Emerg. Technol., vol. 2023, 2023, doi: 10.1155/2023/2103442.

[3] D. Solak and M. Topaloglu, “The Perception Analysis of Cyber Crimes in View of Computer Science Students,” Procedia - Soc. Behav. Sci., vol. 182, pp. 590–595, 2015, doi: 10.1016/j.sbspro.2015.04.787.

[4] F. K. Mupila, H. Gupta, A. University, and A. Bhardwaj, “An Empirical Study on Cyber Crimes and Cybersecurity Awareness,” pp. 1–24, 2023, [Online]. Available: https://doi.org/10.21203/rs.3.rs-3037289/v1

[5] V. Thenmozhi, A. Karunamurthy, and V. Vigneshwar, “Understanding the Dynamics of Cybercrime in India a Comprehensive Study and Recommendations,” vol. 12, no. 7, pp. 168–174, 2023, doi:

10.21275/SR23628155118.
[6] M. Sahat Tobing, U. Wulandari, M. Sari Sihotang, and U. Lancang Kuning, “Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime,” J. Huk. dan Sos. Polit., vol. 1, no. 2, pp. 60–67, 2023.
[7] Navitha. P and Dr. M. Jegadeeshwaran, “An Empirical Study on Cyber Crimes Against Women and Children in India,” Int. J. Adv. Res. Sci. Commun. Technol., pp. 141–149, 2023, doi: 10.48175/ijarsct-11327.
[8] J. Song, “Preschool Cyber Security Management System Based on Intelligent Agents,” Comput. Intell. Neurosci., vol. 2022, 2022, doi: 10.1155/2022/1992429.
[9] R. Y. Patil and S. R. Devane, “Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 5, pp. 2031–2044, 2022, doi: 10.1016/j.jksuci.2019.11.016.
[10] P. R. Yogesh and R. Devane Satish, “Backtracking Tool Root-Tracker to Identify True Source of Cyber Crime,” Procedia Comput. Sci., vol. 171, no. 2019, pp. 1120–1128, 2020, doi: 10.1016/j.procs.2020.04.120.
[11] M. N. Alatawi et al., “Cyber Security against Intrusion Detection Using Ensemble-Based Approaches,” Secur. Commun. Networks, vol. 2023, 2023, doi: 10.1155/2023/8048311.
[12] S. Sumartiningsih, S. S. Pararuk, and N. D. S. Pambudi, “Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime),” J. Dev. Res., vol. 7, no. 1, pp. 95–103, 2023, doi: 10.28926/jdr.v7i1.278.
[13] A. Okutan and Y. Çebi, “A Framework for Cyber Crime Investigation,” Procedia Comput. Sci., vol. 158, pp. 287–294, 2019, doi: 10.1016/j.procs.2019.09.054.
[14] V. I. Tyunin, A. G. Antonov, T. A. Ogar, M. V. Shkele, and E. A. Zorina, “Cyber crimes against property in foreign and Russian criminal law,” SHS Web Conf., vol. 108, p. 02021, 2021, doi: 10.1051/shsconf/202110802021.
[15] S. C. Pawar, R. S. Mente, and B. D. Chendage, “Cyber Crime, Cyber Space and Effects of Cyber Crime,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3307, pp. 210–214, 2021, doi: 10.32628/cseit217139.
[16] S. G. A. van de Weijer and A. Moneva, “Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders,” Comput. Hum. Behav. Reports, vol. 8, no. November, p. 100249, 2022, doi: 10.1016/j.chbr.2022.100249.
[17] N. Wulandari, M. S. Adnan, and C. B. Wicaksono, “Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application,” Hum. Behav. Emerg. Technol., vol. 2022, no. August 2020, 2022, doi: 10.1155/2022/5738969.
[18] A. A. Lodh and C. V. Dalave, “A Study on Types of Cyber Crimes and Cyber Attacks Today,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 2, pp. 220–225, 2022, doi: 10.22214/ijraset.2022.40213.
[19] A. Kumar, “Critical Analysis of the Law Relating to Cyber Crime,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 11, pp. 2081–2082, 2022, doi: 10.22214/ijraset.2022.47771.
[20] E. Sukendy, B. Bayu, and H. Munawar, “Cyber Criminal Policy In The Perspective Of Decency,” Int. Asia Law Money Laund., vol. 1, no. 1, pp. 1–7, 2022, doi: 10.59712/iaml.v1i1.2.
[21] M. Lubis and D. O. D. Handayani, “The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity,” Procedia Comput. Sci., vol. 197, no. 2021, pp. 151–161, 2021, doi: 10.1016/j.procs.2021.12.129.
[22] S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, “Research communities in cyber security: A comprehensive literature review,” Comput. Sci. Rev., vol. 42, p. 100431, 2021, doi: 10.1016/j.cosrev.2021.100431.
[23] H. S. Lallie et al., “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” Comput. Secur., vol. 105, p. 102248, 2021, doi: 10.1016/j.cose.2021.102248.
[24] W. Lin and R. Haga, “Matching Cyber Security Ontologies through Genetic Algorithm-Based Ontology Alignment Technique,” Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/4856265.
[25] X. R. Liu, Y. Meng, and P. Chang, “Node Importance Evaluation of Cyber-Physical System under Cyber-Attacks Spreading,” Complexity, vol. 2021, 2021, doi: 10.1155/2021/6641030.
[26] P. Kotuszewski et al., “Cyber-Security Assessment of Industry 4.0 Enabled Mechatronic System,” Complexity, vol. 2021, 2021, doi: 10.1155/2021/6670625.
[27] S. Tkalichenko, V. Khotskina, Z. Tsymbal, V. Solovieva, and O. Burunova, “Modern Structural Level and Dynamics of Crimes with The Use of Computers, Automation Systems, Computer Networks and Electric Connection Systems,” SHS Web Conf., vol. 100, p. 01014, 2021, doi: 10.1051/shsconf/202110001014.
[28] M. Faisal, I. Ali, M. S. Khan, J. Kim, and S. M. Kim, “Cyber security and key management issues for internet of things: Techniques, requirements, and challenges,” Complexity, vol. 2020, 2020, doi: 10.1155/2020/6619498.
[29] S. Franjić, “Cybercrime is very dangerous form of criminal behavior and cybersecurity,” Emerg. Sci. J., vol. 4, no. Special Issue, pp. 18–26, 2020, doi: 10.28991/esj-2020-SP1-02.
[30] P. Angin, B. Bhargava, and R. Ranchal, “Big Data Analytics for Cyber Security,” Secur. Commun.

Networks, vol. 2019, 2019, doi: 10.1155/2019/4109836.
[31] S. Yan, S. K. Nguang, and L. Zhang, “Nonfragile Integral-Based Event-Triggered Control of Uncertain Cyber-Physical Systems under Cyber-Attacks,” Complexity, vol. 2019, 2019, doi: 10.1155/2019/8194606.
[32] K. A. Ismail, M. M. Singh, N. Mustaffa, P. Keikhosrokiani, and Z. Zulkefli, “Security Strategies for Hindering Watering Hole Cyber Crime Attack,” Procedia Comput. Sci., vol. 124, pp. 656–663, 2017, doi: 10.1016/j.procs.2017.12.202.
[33] Z. Zulkefli, M. M. Singh, A. R. Mohd Shariff, and A. Samsudin, “Typosquat Cyber Crime Attack Detection via Smartphone,” Procedia Comput. Sci., vol. 124, pp. 664–671, 2017, doi: 10.1016/j.procs.2017.12.203.
[34] N. S. Kotwal, “Cyber Crime: A Potential Threat and Remedies,” Int. J. Adv. Res. Ideas Innov. Technol., vol. 3, no. 6, pp. 1281–1284, 2017.
[35] V. Jaganathan, P. Cherurveettil, and P. Muthu Sivashanmugam, “Using a prediction model to manage cyber security threats,” Sci. World J., vol. 2015, 2015, doi: 10.1155/2015/703713.