LatIA. 2024; 2:94
doi: 10.62486/latia202494
ISSN: 3046-403X

ORIGINAL

A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review

Un marco institucional para mejorar la ciberseguridad en la enseñanza superior: Una revisión

Ankit Kumar[1], Khushboo Mishra[2], Rajesh Kumar Mahto[1], Binay Kumar Mishra[2]

[1]Department of Computer Science Veer Kunwar Singh University, Ara, Bihar-802301, India.
[2]P.G. Department of Physics, Veer Kunwar Singh University, Ara, Bihar- 802301, India.

Cite as: Kumar A, Mishra K, Kumar Mahto R, Kumar Mishra B. A Framework for Institution to Enhancing Cybersecurity in Higher Education: A Review. LatIA. 2024; 2:94. https://doi.org/10.62486/latia202494

Submitted: 03-02-2024 **Revised:** 10-05-2024 **Accepted:** 11-09-2024 **Published:** 12-09-2024

Editor: Dr. Rubén González Vallejo

Corresponding author: Ankit Kumar

ABSTRACT

The increasing prevalence of cybersecurity threats has highlighted the urgent need for Higher Education Institutions (HEIs) to prioritize and enhance their cybersecurity measures. This research article presents a comprehensive framework aimed at guiding institutions in strengthening their cybersecurity posture within the higher education sector. The framework addresses the unique challenges faced by HEIs, taking into account the multifaceted nature of cybersecurity and the evolving threat landscape. The proposed framework incorporates a systematic approach that encompasses key components essential for effective cybersecurity management. These components include governance and leadership, risk assessment and management, technical controls, awareness and training, incident response, and collaboration with external stakeholders. The framework emphasizes the integration of these components to establish a robust and holistic cybersecurity strategy. The research article draws upon a thorough review of existing literature, best practices, and industry standards to provide practical insights for HEIs. The framework offers a structured approach that enables institutions to assess their current cybersecurity posture, identify gaps, and implement targeted measures to enhance their overall security resilience. By adopting this framework, institutions can proactively address cybersecurity challenges, mitigate risks, and protect sensitive data and systems. The framework serves as a valuable resource for HEI leaders, policymakers, and cybersecurity professionals seeking to enhance cybersecurity in the higher education landscape.

Keywords: Cybersecurity; Cyber Threats; Higher Education; Mitigate Risks.

RESUMEN

La creciente prevalencia de las amenazas a la ciberseguridad ha puesto de relieve la urgente necesidad de que las Instituciones de Educación Superior (IES) prioricen y mejoren sus medidas de ciberseguridad. Este artículo de investigación presenta un marco integral destinado a guiar a las instituciones en el fortalecimiento de su postura de ciberseguridad dentro del sector de la educación superior. El marco aborda los retos específicos a los que se enfrentan las IES, teniendo en cuenta la naturaleza polifacética de la ciberseguridad y la evolución del panorama de las amenazas. El marco propuesto incorpora un enfoque sistemático que abarca componentes clave esenciales para una gestión eficaz de la ciberseguridad. Estos componentes incluyen gobernanza y liderazgo, evaluación y gestión de riesgos, controles técnicos, concienciación y formación, respuesta a incidentes y colaboración con partes interesadas externas. El marco hace hincapié en la integración de estos componentes para establecer una estrategia de ciberseguridad sólida y holística. El artículo de investigación se basa en una revisión exhaustiva de la literatura existente, las mejores prácticas y las normas de la industria para proporcionar ideas prácticas para las IES. El marco ofrece un enfoque estructurado que permite a las instituciones evaluar su postura actual en materia de ciberseguridad, identificar lagunas y aplicar medidas específicas para mejorar su resistencia general en materia de seguridad. Al adoptar este marco, las instituciones pueden abordar de forma proactiva los retos de la ciberseguridad, mitigar los riesgos y proteger los datos y sistemas sensibles. El marco constituye un valioso recurso para los dirigentes de las IES, los responsables políticos y los profesionales de la ciberseguridad que deseen mejorar la ciberseguridad en el ámbito de la enseñanza superior.

Palabras clave: Ciberseguridad; Ciberamenazas; Enseñanza Superior; Mitigar Riesgos.

INTRODUCTION

In recent years, the exponential growth of cybersecurity threats has been fueled by advancements in cutting-edge technologies like artificial intelligence (AI) and the Internet of Things (IoT). This ever-evolving landscape of cyber threats has imposed a significant burden on organizations, as the methods and objectives of these threats continue to evolve at a rapid pace. While cybersecurity challenges affect virtually every major industry, the higher education sector stands out as particularly susceptible to such vulnerabilities. The security vulnerabilities present in higher education can be attributed to multiple factors. Firstly, the repercussions of cyberattacks go beyond mere financial losses within the realm of higher education. This is because higher education institutions (HEIs) store a significant amount of sensitive data, including personal records of students, valuable research data, and intellectual properties that are crucial to their operations. As a result, protecting this vast volume of sensitive information becomes paramount to ensuring the security and integrity of higher education systems.(1)

The potential consequences of information loss or compromise within higher education are severe, as they not only pose a significant threat to individuals but also have the potential to inflict substantial damage on a university's reputation. Additionally, higher education institutions often serve as hosts for critical infrastructure and user-intensive systems that are essential for the functioning of a nation or city. Therefore, any cybersecurity incidents targeting these institutions could have disastrous implications.(3) Furthermore, in comparison to business corporations, the IT systems of many higher education institutions exhibit a decentralized structure. This decentralized structure is often a result of individual faculties or departments operating under their own IT structures, which aligns with their diverse technological requirements from an operational standpoint.

Nevertheless, this fragmented configuration introduces explicit security vulnerabilities that can be exploited by malicious attackers. Moreover, the distinctive culture of academia, which values a certain level of openness and transparency not commonly found in other industries, further contributes to these security vulnerabilities. Higher education institutions (HEIs) have traditionally embraced a design that promotes accessibility to the public, aligning with their mission of knowledge dissemination. However, this accessibility also implies that their networks are as open as their physical campuses, thereby posing additional security challenges.

Lastly, with the unprecedented transition to remote work and online learning prompted by the COVID-19 pandemic in 2020, a greater number of personal devices not supplied by the university are now connecting to the network and IT systems of higher education institutions (HEIs). As a result, the importance of cybersecurity has reached an unprecedented level, given the heightened risks and implications associated with safeguarding these expanded digital landscapes.(4)

As a result of these vulnerabilities, there is an increased focus on cybersecurity within higher education institutions (HEIs). This heightened attention is exemplified by the introduction of a new Horizon Report dedicated to Information Security in 2021.(5) In the midst of this, higher education institutions (HEIs) are actively investing in talent and infrastructure to effectively address the ever-evolving cybersecurity challenges. Consequently, institutional leaders and policy-makers are seeking strategies that prioritize resources and efforts to tackle this critical issue. However, existing research on cybersecurity often lacks practical value for these leaders and policy-makers, as it predominantly focuses on technology. Moreover, publications highlighting best practices frequently overlook the holistic, system-wide perspective needed for cybersecurity in HEIs. Recognizing this literature gap, our paper aims to bridge this divide by exploring institutional strategies for cybersecurity in HEIs from a comprehensive system perspective. By doing so, we aspire to provide valuable insights and actionable recommendations that can assist HEI leaders and policy-makers in their pursuit of effective cybersecurity strategies.

Types of cyberattacks

Cyberattacks are malicious activities that target computer systems, networks, and digital infrastructure with the intention of gaining unauthorized access, causing damage, or extracting valuable information. There are several types of cyberattacks, each with its own characteristics and objectives. Here are some common types of cyberattacks:

- *Malware Attacks*: Malware, short for malicious software, refers to any software designed to harm or exploit a computer system. This includes viruses, worms, ransomware, spyware, and Trojans. Malware attacks typically involve the installation of malicious software without the user's knowledge or consent, which can lead to data breaches, system disruption, or unauthorized access.[1]
- *Phishing Attacks*: Phishing attacks aim to trick individuals into revealing sensitive information such as login credentials, credit card numbers, or personal data. Attackers often impersonate legitimate entities, such as banks or popular websites, and use deceptive emails, messages, or websites to lure victims into providing their information.
- *Denial-of-Service (DoS) Attacks:* DoS attacks seek to overwhelm a target system or network with a flood of traffic, rendering it unavailable to legitimate users. These attacks disrupt the normal functioning of a system or network by consuming its resources, causing service disruptions or complete shutdowns.

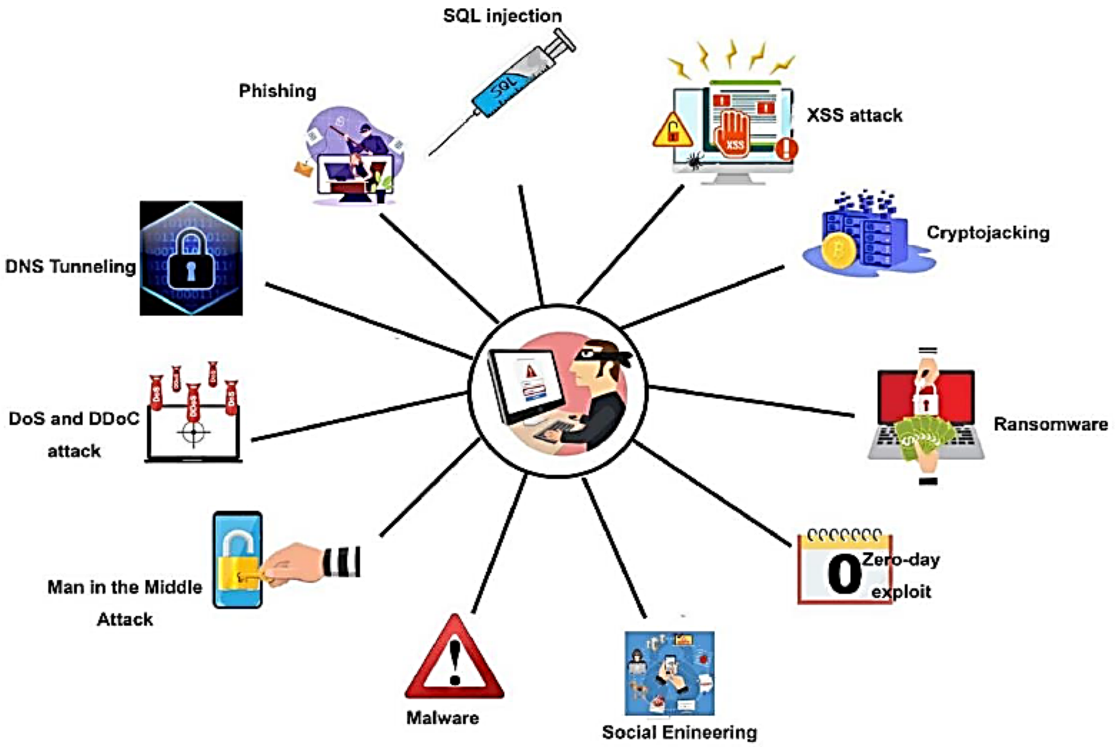

Figure 1. Types of cyberattacks

- *Man-in-the-Middle (MitM) Attacks*: MitM attacks occur when an attacker intercepts and alters communications between two parties without their knowledge. By eavesdropping on or manipulating the communication flow, the attacker can gain access to sensitive information, including passwords, financial details, or confidential data.
- *SQL Injection Attacks*: SQL injection attacks exploit vulnerabilities in web applications that use a database backend. By injecting malicious SQL code into input fields, attackers can manipulate database queries and gain unauthorized access to sensitive information or even modify the underlying database.
- *Social Engineering Attacks*: Social engineering attacks exploit human psychology rather than technical vulnerabilities. These attacks manipulate individuals into divulging confidential information, such as passwords or access codes, by taking advantage of trust, authority, or a sense of urgency.
- *Insider Threats*: Insider threats involve attacks or data breaches caused by individuals within an organization who have authorized access to sensitive data. These individuals may misuse their privileges or intentionally leak information, causing significant harm to the organization's security and reputation.

It's important to note that cyberattacks are continually evolving, with attackers employing increasingly sophisticated techniques. Organizations and individuals must stay vigilant, employ robust cybersecurity measures, and regularly update their defenses to protect against the ever-changing threat landscape.[7]

This article initially examines the evolutionary trajectory of the cybersecurity landscape over the past few decades, identifying the latest trends and projections for the upcoming decade. By delving into these historical advancements and emerging shifts, we emphasize the criticality of revisiting cybersecurity issues within higher education institutions (HEIs). Through an exploration of the formidable challenges faced by HEIs in combating the ever-growing wave of cyberattacks, we advocate for a comprehensive, system-wide approach to fortify HEI cybersecurity, underscoring the need to reevaluate areas of priority. Drawing upon an extensive literature review and thorough desk research, which explores methodologies capable of mitigating cybersecurity vulnerabilities in the coming decade, we amalgamate our findings to present a collection of institutional strategies accompanied by practical takeaways. These strategic insights are intended to empower HEIs in fortifying their resilience against cybersecurity threats as they navigate the future.(8,9)

Literature review

A systematic literature review on information security management in higher education" by Bongiovanni presents a systematic literature review on information security management within higher education institutions (HEIs). The study aims to explore the current state of information security practices in the higher education sector and identify potential gaps and challenges. The author conducts a comprehensive review of relevant literature published up to 2019, encompassing various aspects of information security management in higher education. One of the key strengths of this paper is its systematic approach to reviewing the literature. By employing a systematic methodology, the author ensures the inclusion of a wide range of sources and provides a comprehensive overview of the research landscape in this domain. This systematic review methodology enhances the credibility and reliability of the findings. The paper highlights several important themes and insights derived from the reviewed literature. It identifies common challenges faced by HEIs, such as the lack of resources and expertise, the complexity of managing security in decentralized environments, and the need for a balance between security and academic openness. These findings contribute to a better understanding of the unique information security management issues specific to higher education institutions. Bongiovanni's paper provides a valuable contribution to the literature on information security management in higher education institutions. By conducting a systematic review, the paper offers a comprehensive overview of the current state of information security practices in the higher education sector.(10,11) The identified challenges and insights can guide policymakers, administrators, and security professionals in developing effective strategies to enhance information security in higher education institutions. Researchers and practitioners in the field can benefit from the paper's findings as a foundation for further research and practical implementation in the evolving landscape of information security.

Kwaa-Aidoo and Agbeko investigates the information system security practices within a specific Ghanaian university. The authors begin by highlighting the increasing importance of information system security in educational institutions, given the rising threat landscape and the critical nature of the data stored and processed within universities. The focus on a specific Ghanaian university adds a valuable perspective to the literature, as it provides insights into the unique challenges faced by universities in developing countries. The paper adopts a research methodology that combines both qualitative and quantitative approaches. The authors conduct interviews, surveys, and observations to gather data on the university's information system security practices. This multi-method approach enhances the robustness and reliability of the findings by capturing different perspectives and sources of information. One of the notable strengths of this paper is the in-depth analysis of the information system security practices in the selected Ghanaian university. The authors identify and discuss various security measures implemented by the university, including policies, access controls, authentication mechanisms, incident response procedures, and awareness programs. This comprehensive analysis provides valuable insights into the existing security measures and their effectiveness in mitigating potential risks. Furthermore, the paper highlights the vulnerabilities and challenges identified during the analysis. It discusses issues such as weak passwords, inadequate employee training, lack of security awareness, and limited resources. By identifying these vulnerabilities, the authors contribute to raising awareness of the specific areas that require improvement within the context of the studied Ghanaian university. Kwaa-Aidoo and Agbeko's paper provides a valuable analysis of the information system security practices in a Ghanaian university. The combination of qualitative and quantitative research methods, along with the in-depth analysis and recommendations, makes this paper a valuable contribution to the field. The findings and recommendations can guide universities in Ghana and other similar contexts in strengthening their information system security posture. Further research can build upon this study by exploring additional universities and considering the evolving landscape of information security.

Pinheiro begin by emphasizing the increasing significance of cybersecurity in educational institutions due to the growing dependence on technology and the abundance of sensitive data. The paper focuses on providing an overview of cyber threats specifically targeting educational institutions, highlighting the unique challenges faced by this sector. One of the notable strengths of this paper is the inclusion of diverse cyber threats and attack vectors specific to educational institutions. The authors discuss various types of cyber threats such as ransomware attacks, phishing attempts, data breaches, DDoS attacks, and insider threats. By providing an extensive review of these threats, the paper contributes to raising awareness and understanding among educational institutions regarding the potential risks they face. The paper also addresses the impact of cyber threats on educational institutions. It discusses the potential consequences of successful cyber attacks, including disruption of services, compromised sensitive data, financial losses, reputational damage, and hindrance to the educational process. By highlighting the ramifications of cyber threats, the authors emphasize the urgency for educational institutions to prioritize cybersecurity measures. Furthermore, the paper presents an analysis of mitigation strategies to combat cyber threats in educational institutions. It discusses the importance of adopting a multi-layered security approach, implementing security awareness programs, conducting regular risk assessments, establishing incident response plans, and enhancing technical defenses. These strategies provide practical insights for educational institutions to strengthen their cybersecurity posture.

However, it is important to note that the publication date of this paper is in 2020, and the rapidly evolving nature of cyber threats means that some of the information and examples provided may not reflect the most current landscape. It would be beneficial for future research to consider the evolving threat landscape and include recent case studies and emerging cyber threats. Pinheiro's paper provides a valuable review of cyber threats targeting educational institutions. The comprehensive analysis of various cyber threats, their impact, and suggested mitigation strategies offers valuable insights for educational institutions seeking to enhance their cybersecurity measures. The paper serves as a foundation for understanding the specific challenges faced by educational institutions and can guide the development of effective cybersecurity strategies. Further research can build upon this review by considering the evolving threat landscape and exploring emerging technologies and trends in cybersecurity for educational institutions.

Approach to Tackling Cybersecurity Challenges in Higher Education Institutions

Although there is no universally applicable solution or quick fix for cybersecurity, there exist strategies that can assist higher education institutions (HEIs) in effectively addressing their cybersecurity challenges in a sustainable manner. Departing from a narrow focus on technology, we put forth a comprehensive system-wide approach aimed at safeguarding HEI cybersecurity. Through an in-depth analysis and extensive desk research [12] of the existing literature and promising practices, we consolidate our findings to offer a collection of recommendations for institutional strategies. These recommendations are tailored to empower HEIs to proactively tackle the evolving cybersecurity landscape and prepare them to effectively mitigate future threats.[13]

Strengthening Institutional Governance for Cybersecurity

According to scholars, a governance approach to organizational cybersecurity, encompassing leadership, organizational structures, and processes, has been recommended. This approach emphasizes the need for senior management to prioritize cybersecurity and actively engage in its oversight. Apart from senior management involvement, the commitment and attitude of leadership play a critical role. Furthermore, it is essential for leadership to recognize that cybersecurity is not solely the responsibility of IT departments but should be a focal point of institution-wide endeavors.[14] As digital technologies are aligned with business strategy, a similar alignment should be established with cybersecurity. It is imperative to integrate cybersecurity into the broader governance framework and ensure its integration across the organization.

Training and Cybersecurity Awareness Campaigns to Build Cybersecurity Culture

Higher education institutions (HEIs) must acknowledge the vulnerability of human factors within the contemporary cybersecurity landscape.[15,16] Scholars and experts in cybersecurity have underscored the importance of cultivating a cybersecurity culture as a means to reshape attitudes, perceptions, and foster positive security behaviors. Establishing a cybersecurity culture is vital not only for instilling good practices but also for facilitating the effective implementation of security plans and policies. By promoting a culture of cybersecurity awareness, HEIs can enhance their overall security posture and mitigate the risks posed by human vulnerabilities. In line with the practices identified by Alshaikh, fostering a cybersecurity culture within HEIs can be accomplished through training programs and cybersecurity awareness campaigns.[17,18] Particularly, it is crucial to provide staff members who handle personal data in HEIs with comprehensive awareness training and consistent updates to ensure the protection of entrusted data. Defining and documenting appropriate roles and responsibilities for staff members at different levels aligns with the institution's security policy and enhances overall security measures. By implementing these measures, HEIs can effectively strengthen their cybersecurity culture and mitigate potential risks associated with data handling.

It is imperative for staff members to recognize that cybersecurity is a collective responsibility, and adhering to best practices should be the standard norm.[17,18] Creating a culture of organizational cybersecurity awareness can begin right from the employee onboarding process. All new hires should be actively engaged in orientation workshops where they are equipped with essential information, including security policies, procedures, and the consequences of security breaches. By instilling this knowledge from the beginning, organizations can foster a proactive mindset among employees, ensuring that cybersecurity remains a priority throughout their tenure. To enhance content absorption and comprehension, it is essential to ensure that these workshops prioritize a human-centric approach.(21) Simultaneously, new employees should be obligated to sign an acknowledgement form, signifying their thorough reading and comprehension of the institution's security policies. By acknowledging the gravity of information security concerns within the institution, employees demonstrate their commitment to safeguarding and proactively responding to cybersecurity challenges, both within and beyond their designated work responsibilities. This process solidifies their dedication to upholding the highest standards of cybersecurity and strengthens the overall security posture of the organization.

Introduction of New and More Sophisticated Security Measures

Implementing a single sign-on (SSO) system enables users to authenticate themselves once, granting them subsequent access to multiple applications within or across an institution's IT systems. This eliminates the necessity for separate logins that involve individual usernames and passwords, thereby reducing the likelihood of security breaches resulting from lost, forgotten, or stolen credentials. SSO streamlines the authentication process, enhancing both user convenience and overall cybersecurity by minimizing the vulnerabilities associated with multiple login credentials. Ensuring identity assurance involves verifying the true identity of an individual rather than solely relying on a password, which is often insufficient. To strengthen this process, an additional layer of factors is required to validate one's identity. Multi-factor Authentication (MFA) is an authentication approach that necessitates individuals to provide two or more pieces of evidence to confirm their identity, granting them access to the system. By implementing MFA, organizations enhance the security of their systems by requiring multiple forms of authentication, thereby reducing the risks associated with unauthorized access and identity impersonation.(20,21)

While adaptive authentication has not reached a stage where it is fully ready for widespread adoption in HEIs, it offers a promising avenue for exploration in mitigating risks associated with human factors and data-related vulnerabilities. HEIs can consider this approach as they seek effective strategies to address the challenges posed by evolving cybersecurity threats. By adapting authentication mechanisms based on contextual factors and user behavior, adaptive authentication holds the potential to enhance the security posture of HEIs and provide a proactive defense against emerging risks. Continued research and development in this area can pave the way for its future implementation in higher education institutions.

CONCLUSIONS

The rapid adoption of emerging technologies in the digital landscape brings along heightened vulnerabilities. As a result, HEIs face ongoing challenges from novel cyber-attacks that continuously probe their cybersecurity capabilities. In order to effectively address the evolving cybersecurity risks of the new decade, and considering the distinctive characteristics of HEIs that may limit the suitability of conventional organizational cybersecurity management approaches, this research puts forward a comprehensive system-wide approach accompanied by prioritized institutional strategies. While the strategies outlined above may not offer a foolproof solution and cannot guarantee protection against every possible attack, they do provide a system-wide approach that offers tangible advantages in the battle against cyber threats within higher education. By adopting these strategies and engaging all relevant stakeholders, we are confident that cybersecurity can be effectively maintained throughout the upcoming decade. It is crucial to thoroughly evaluate and implement these strategies in a collaborative manner, ensuring the collective effort of HEI stakeholders in safeguarding against potential cyber threats. In order to gauge the effectiveness of these strategies, future research endeavors can focus on conducting empirical studies. By examining their implementation and impact within diverse HEI contexts, we can gain valuable insights into the strategies' applicability. Such investigations would contribute to a deeper understanding of the strategies' efficacy and provide valuable guidance for their potential refinement and optimization in different higher education settings.

REFERENCES

1. Banks W. Cyber attribution and state responsibility. Int Law Stud. 2021;97(1):43.

2. Alsmadi I, Easttom C. The NICE Cyber Security Framework. Springer; 2020.

3. Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv Prepr arXiv190102672. 2019;

4. Haque MA, Haque S, Kumar K, Singh NK. A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. In: Digital Transformation and Challenges to Data Security and

Privacy. IGI Global; 2021. p. 63-90.

5. Goutam RK. Importance of cyber security. Int J Comput Appl. 2015;111(7).

6. Sarker IH. CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things. 2021;14:100393.

7. Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, Singh S. A review on cyber crimes on the Internet of Things. arXiv Prepr arXiv200905708. 2020;

8. Haque MA, Amola Y, Singh NK. Threat Analysis and Guidelines for Secure WiFi and WiMAX Network. 2011;

9. Haque MA, Amola Y, Singh DNK. Performance of Wimax over Wi-Fi with Reliable QoS over Wireless Communication Network. World Appl Program J. 2011;1.

10. Prakash A, Haque A, Islam F, Sonal D. Exploring the Potential of Metaverse for Higher Education: Opportunities, Challenges, and Implications. Metaverse Basic Appl Res [Internet]. 2023 Apr 26;2(SE-Reviews):40. Available from: https://mr.saludcyt.ar/index.php/mr/article/view/40

11. Haque MA, Sonal D, Haque S, Rahman M, Kumar K. Learning management system empowered by machine learning. In 2022. p. 020085. Available from: http://aip.scitation.org/doi/abs/10.1063/5.0074278

12. Corallo A, Lazoi M, Lezzi M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Comput Ind. 2020;114:103165.

13. Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. J Big data. 2020;7:1-29.

14. Ali S, Bosche A, Ford F. Cybersecurity is the key to unlocking demand in the internet of things. Bain Co Boston, MA, USA. 2018;

15. Md. Alimul Haque, Anil Kumar Sinha MUB and NKS. Comparative study on Wireless threats and their Classification. In 2017. Available from: http://bvicam.in/INDIACom/news/INDIACom 2017 Proceedings/Main/papers/2511.pdf

16. Md Alimul HaqueA.K.SinhaNidhi RajN.K.Singh. Wi-Fi adoption and security survey. J Electr Electron Eng. 2017;

17. Hossain MA, Haque MA, Ahmad S, Abdeljaber HAM, Eljialy AEM, Alanazi A, et al. AI-enabled approach for enhancing obfuscated malware detection: a hybrid ensemble learning with combined feature selection techniques. Int J Syst Assur Eng Manag [Internet]. 2024; Available from: https://doi.org/10.1007/s13198-024-02294-y

18. Haque MA, Ahmad S, Sonal D, Abdeljaber HAM, Mishra BK, Eljialy AEM, et al. Achieving Organizational Effectiveness through Machine Learning Based Approaches for Malware Analysis and Detection. Data Metadata. 2023;2:139.

19. Haque A, Sinha AK, Singh KM, Sing NK. Security Issues of Wireless Communication Networks. IJECCE. 2014;5(5):1191-6.

20. Haque MA, Haque S, Zeba S, Kumar K, Ahmad S, Rahman M, et al. Sustainable and efficient E-learning internet of things system through blockchain technology. E-Learning Digit Media [Internet]. 2023;0(0):1-20. Available from: https://journals.sagepub.com/doi/abs/10.1177/20427530231156711

21. Haque S, Zeba S, Alimul Haque M, Kumar K, Ali Basha MP. An IoT model for securing examinations from malpractices. Mater Today Proc. 2021 Apr;

22. Haque S, Haque MA, Kumar D, Mishra K, Islam F, Ahmad S, et al. Assessing the Impact of IoT Enabled E-Learning System for Higher Education. SN Comput Sci [Internet]. 2023;4(5):459. Available from: https://doi.

org/10.1007/s42979-023-01860-8

23. Almrezeq N, Haque MA, Haque S, El-Aziz AAA. Device Access Control and Key Exchange (DACK) Protocol for Internet of Things. Int J Cloud Appl Comput [Internet]. 2022 Jan;12(1):1-14. Available from: https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJCAC.297103

ACKNOWLEDGMENT

We thank to all authors.

AVAILABILITY OF DATA AND MATERIALS

The datasets used in this research are publicly available and properly cited in our dataset section for transparency and ease of replication.

COMPETING INTERESTS SECTION

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

FINANCING

None.

CONFLICT OF INTEREST

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

AUTHOR CONTRIBUTIONS

Conceptualization: Ankit Kumar, Khushboo Mishra, Rajesh Kumar Mahto and Binay Kumar Mishra.

Investigation: Ankit Kumar, Khushboo Mishra, Rajesh Kumar Mahto and Binay Kumar Mishra.

Methodology: Ankit Kumar, Khushboo Mishra, Rajesh Kumar Mahto and Binay Kumar Mishra.

Writing - original draft: Ankit Kumar, Khushboo Mishra, Rajesh Kumar Mahto and Binay Kumar Mishra.

Writing - review and editing: Ankit Kumar, Khushboo Mishra, Rajesh Kumar Mahto and Binay Kumar Mishra.