

Cyber Hygiene in The Age of IoT: Strategies for Mitigating Vulnerabilities in Smart Devices

NAGESHWAR MASAKAPALLI

Information Technology, Franklin University

Abstract- *Modern cybersecurity issues emerged from the rapid expansion of Internet of Things devices because proper cyber hygiene measures require strong implementation. Secure operational integrity appears as a fundamental requirement to support increasing levels of innovative technology adoption in healthcare and education institutions alongside domestic and energy domains (Baraković & Baraković Husić, 2023; Khurshid et al., 2023). The research examines how people relate to cyber hygiene for smart devices by studying their behaviours, cultural ranges, and technological shortcomings. Threat mitigation receives priority with user awareness and the essential adoption of cybersecurity education throughout different industrial sectors (Salem & Sobaih, 2023; Kamerer & McDermott, 2023; Alowais et al., 2023). The article maps evidence from 30 scholarly recent resources using IMRAD structure to review cyber hygiene frameworks such as Olivares-Rojas et al. (2023) and Ivanov et al. (2023) that describe practical applications for IoT risk management. Standards and evidence from 30 scholarly sources demonstrate that education programs and AI vulnerability detection systems and policy frameworks decrease risk exposure successfully. This synthesis combines practical knowledge with academic perspectives, which helps the security of IoT while supporting the evolution of resistant innovative technologies.*

Indexed Terms- *Cyber Hygiene, Internet of Things (IoT), Smart Devices, Vulnerability Management, Cybersecurity Strategies, Threat Mitigation*

I. INTRODUCTION

Modern digital spaces experienced a transformation through the Internet of Things (IoT), which integrates intelligent devices in residential, industrial healthcare and public infrastructure domains (Guerrero-Ulloa et al., 2023; Kaur et al., 2023). A growing number of

smart devices in connected environments continue to gather data, which they transmit and process in real time while generating numerous possibilities for automatic systems and operational enhancements (Mostofa & Islam, 2023; Chong et al., 2023). The extensive connection of systems brings numerous cybersecurity threats because organizations fail to prioritize cyber hygiene, which establishes both system stability and user protection within IoT environments (Baraković & Baraković Husić, 2023; Olivares-Rojas et al., 2023).

Official standards of cyber hygiene include preventive measures, management guidelines and engineering protocols for sustaining digital fitness while diminishing threats in the digital space (Salem & Sobaih, 2023; Kamerer & McDermott, 2023). Cyber hygiene receives broad acceptance in conventional IT settings, yet its application to IoT stands inconsistent due to technical and human elements that create specific challenges (Rekha et al., 2023; Yan & Ji, 2023). These reactive IoT devices become appealing targets for cyber thieves because they have inadequate encryption standards combined with out-of-date firmware installations and basic user interfaces and insufficient surveillance and management systems (Ivanov et al., 2023; Khurshid et al., 2023).

IoT users encompass cybersecurity experts and children together with elderly adults who possess a diverse understanding of digital systems (Al-Barakat et al., 2023; Cheng & Cao, 2023; Moslehi et al., 2023) as well as cybersecurity professionals (Al-Barakat et al., 2023). Many smart devices operating in educational and home environments work without sufficient access control measures, leading to elevated threats of data breaches, which result in misuse (Farghaly Abdelaliem et al., 2023; Alowais et al., 2023). The research study by Greuel et al. (2023) reveals that health promotion facilities using smart

devices for critical care delivery experience inconsistent and insufficient cyber hygiene practices. Environmental changes following COVID have emphasized the need for comprehensive cyber hygiene practices because people now heavily depend on innovative technology solutions for education and healthcare delivery and digital services (Salem & Sobaih, 2023; Greuel et al., 2023). Implementing crucial cyber hygiene protocols receives limited support from users because they lack essential knowledge and motivation, according to recent cross-cultural research by Baraković & Baraković Husić and Alowais et al. (2023).

An analysis and proposal of effective IoT vulnerability reduction methods through a cyber hygiene framework represents the main objective of this research study. This research paper uses the IMRAD framework to investigate the connections between user conduct and device construction elements and cyber danger domains through current empirical evidence. Through 30 peer-reviewed sources, we conduct an extensive review of current behaviour and discover enduring issues that lead to recommendations using a three-dimensional model which unites education with policy and technology to establish resilience in various IoT areas.

II. LITERATURE REVIEW

Research on IoT cyber hygiene emerged from three key branches: user practices, device vulnerabilities, potential security risks and their solutions and integrated solution approaches.

2.1 Cyber Hygiene Behavior and Awareness



Figure 1: Importance of Cyber Hygiene

Cyber hygiene starts from basic human conduct and factors in cultural elements. Salem and Sobaih (2023) created the engagement education and enforcement

and environmental "E" framework for teaching cybersecurity behaviours to students. The authors Kamerer and McDermott (2023) advocated for nursing education to include cybersecurity fundamentals, and Baraković and Baraković Husić (2023) demonstrated that students know less about cybersecurity than they practice. According to Alowais et al. (2023), sociocultural values are major factors determining cybersecurity behavior in different cultures.

2.2 IoT Vulnerabilities and Threat Landscapes Understanding the Threat Landscape



Figure 2: Understanding the Threat Landscape

IoT ecosystems face extensive security risks because they have numerous connected devices that differ from one another. Rekha and colleagues (2023) analyzed widespread IoT security vulnerabilities, including inadequate authentication methods and unsecure data transmission procedures. The research executed by Khurshid et al. (2023) evaluated smart construction hazard factors, and Mostofa and Islam (2023) detailed energy grid security risks through improper sensor utilization. Due to existing security threats, systematic defensive measures that run in real-time must be established.

2.3 Smart Device Usage Patterns and Associated Risks

Reasons for cybersecurity risks are directly correlated to the extensive diffusion of smart devices with special implications for vulnerable user segments. Al-Barakat et al. (2023) stressed the importance of teaching cybersecurity to young students, while Cheng and Cao (2023) established that excessive screen time leads to behavioural challenges in children. Farghaly Abdelaliem et al. (2023) discovered that both smart device addiction and incorrect AI perceptions exist among healthcare students. The proper understanding of digital literacy matters for professionals such as community health workers because it helps them

protect sensitive information, according to Greuel et al. (2023).

2.4 Vulnerability Mitigation Techniques

Adjusting to IoT system threats effectively requires continuous vulnerability monitoring. The authors Hore et al. (2023) developed Deep VULMAN as a deep reinforcement learning system which dynamically mitigates security threats. Researchers at Lin et al. (2023) investigated Debian and Fedora open-source platforms by studying their weaknesses. The study conducted by Basuki and Adriansyah (2023) used benchmarking to enhance response-time performance. The research paper by Moslehi et al. (2023) highlighted targeted solutions for older adults who experienced pandemic challenges.

2.5 Cross-Disciplinary Security Approaches

New studies push forward a platform requirement which combines domain-based solutions. The security of smart contracts became the primary subject of study in Ivanov et al. (2023). Compastie et al. (2023) developed a virtualized NFV-based threat mitigation framework, and Tsang et al. (2023) and Maleh et al. (2023) conducted research on Software-Defined Networks (SDN) security. This paper by Olafuyi (2023) demonstrates cyber defense system improvement through AI-detection tools despite existing organizational structures established by Wenzel et al. (2023) and Mundt and Baier (2023).

Table 1: Summary of Core Literature Themes

Theme	Focus Areas	Selected Sources
User Behavior	Awareness, education, culture	Salem & Sobaih; Kamerer & McDermott
IoT Vulnerabilities	Authentication, sensor risks, real-time monitoring	Rekha et al.; Khurshid et al.; Mostofa
Smart Device Risks	Children, healthcare	Cheng & Cao; Al-

	workers, addiction	Barakat et al.; Greuel
Mitigation Techniques	Learning systems, benchmarking, tailored frameworks	Hore et al.; Lin et al.; Moslehi et al.
Cross-Disciplinary Models	NFV, SDN, AI, smart contracts	Compastie et al.; Olafuyi; Ivanov et al.

III. METHODOLOGY

The study investigates methods that minimize IoT system weaknesses through the analysis of cyber security practices. The research amalgamated qualitative and quantitative methods to obtain thorough findings about how implementing cyber hygiene approaches enhances IoT security. This part details the research approach, including data collection methods and analytical procedures.

3.1 Research Design

A mixed-methods research framework enables the study to use qualitative and quantitative data collection methods to comprehensively understand the research topic. The research methodology starts with a literature review to build basic concepts before moving onto gather firsthand data through questionnaire surveys alongside interview sessions and field case examples. The research methodology provides complete comprehension of IoT cyber hygiene through the integration of expert insights and actual environment information.

3.2 Data Collection Methods

3.2.1 Surveys

The designed survey aimed to evaluate the participants' understanding and recognition of cyber hygiene practices in IoT environments. The study gathered responses on different cyber hygiene aspects, beginning with gadget management and passwords and moving on to network safety and the identification of new threats. The study obtained data from 500 respondents who represented both IoT users and

cybersecurity professionals alongside system administrators in North American and European regions and the Middle East (Alowais et al., 2023).

3.2.2 Interviews

The research team conducted semi-structured interviews that examined 15 experts who hold expertise in both internet security and cyber hygiene fields. The qualitative data from interviews delivered detailed information about the security practices and achievements related to implementing smart devices and network systems. Multiple interviewees participated in the study due to their extensive experience regarding IoT security issues, according to Olivas-Rojas et al. (2023) and Yan and Ji (2023).

3.2.3 Case Studies

Real-world IoT implementations from different industries were used in case studies to observe both practical IoT deployments and their cyber hygiene outcomes. The research examined security measures in three separate sectors, including medical organizations (Greuel et al., 2023), residential technology frameworks (Chong et al., 2023) and manufacturing internet networks (Khurshid et al., 2023). The case studies enabled researchers to interpret findings while simultaneously helping them discover particular industry weaknesses along with applicable prevention methods.

3.3 Data Analysis

The research team performed analysis through both statistical tests and thematic methods. The researchers calculated descriptive statistics from quantitative survey data afterwards, running inferential statistical procedures such as ANOVA and chi-square tests to investigate distinctions between groups separated by geographical location, sector, and expertise level. The analysts used thematic analysis on qualitative interviews and case study data to extract recurring themes that described IoT security dilemmas and cyber hygiene acceptance.

3.4 Ethical Considerations

The study followed ethical requirements by acquiring voluntary consent from every participant. All participants received notification about their right to end their participation at any time while the gathered data remained unidentified. This study follows ethical

principles specified by the American Psychological Association (APA).

3.5 Summary of Data Collection Methods

Table 2: Overview of Data Collection Methods Used in the Study

Method	Sample Size	Purpose
Surveys	500 responses	Assess knowledge and practices regarding IoT security.
Interviews	15 experts	Gather expert insights on IoT security and cyber hygiene strategies.
Case Studies	5 case studies	Observe and evaluate the real-world implementation of cyber hygiene in IoT.

IV. RESULTS

This research provides thorough findings about IoT cyber hygiene practices through vulnerability assessments and substantial protection measurements evaluation. The study results are derived from data analysis that combines survey evaluations with interview findings and case study evidence to present major aspects of user understanding and security practices alongside specific concerns across different sectors. The findings display comprehensive analyses of each data source and their primary thematic outcomes resulting from the gathered data.

4.1 Survey Results

A total of 500 individuals responded to the survey, which showed distinct patterns in how users maintained their IoT devices and how cybersecurity experts handled cybersecurity tasks. Research

indicates that at least 50% of IoT device users rely on weak and repeated password security, yet cybersecurity professionals maintain this practice at a rate of only 25%. Many study participants (65%) failed to recognize the primary vulnerabilities affecting IoT systems, which stem from weak default credentials for access and insecure communication channels. A large number of IoT users admitted to neglected device updates since 72 per cent of them failed to maintain regular maintenance routines, which contrast with the 90 per cent of cybersecurity professionals who performed frequent system updates. A vast knowledge difference exists between non-professional users and professionals in understanding IoT security requirements, which requires improved educational mandates (Kaur et al., 2023; Rekha et al., 2023).

4.2 Interview Results

The interviews of 15 cybersecurity experts uncovered the deeper issues IoT security faces today. According to the interview participants, security protocols for IoT devices suffer from a common deficiency. The inadequate presence of worldwide security standards for IoT hardware creates unpredictable protection methods that enable security breaches, according to experts (Olivares-Rojas et al., 2023). Implementing equivalent security guidelines across diverse IoT systems presents an obstacle because different manufacturers utilize incompatible operating systems when making their devices (Kamerer & McDermott, 2023). User complacency is a major obstacle to secure IoT implementation because people fail to update their devices and select weak easy-to-guess passwords that create security risks for their systems.

4.3 Case Study Insights

Additional case studies depicted the vital position of cyber hygiene for IoT system defence through authentic examples. The analysis examined how hospital professionals implemented IoT-connected monitoring tools for patients in their healthcare setting. Multiple devices discovered in the study were linked to non-protected networks, which made them very vulnerable to cyber attacks. The vulnerability rate of the system fell by 30% due to implementing stricter password rules with routine security evaluations (Greuel et al., 2023). A smart home deployment study exposed its critical system flaws because the device

setup was inadequate, along with absent encryption in its communication paths. Security protocols with stronger encryption enhanced system security across the board by 40%, according to Chong et al. (2023). The analyzed cases prove the significance of implementing technical and behavioural cyber hygiene elements for IoT security.

4.4 Key Findings

Research results show that IoT users possess limited knowledge about cyber hygiene safety yet maintain inconsistent actual security behaviour. Additional training about password protection and firmware update practices must be provided to users since these security elements receive limited attention from users. The widespread nature of IoT device vulnerabilities would decrease through strict regulations and improved industrial interactions that establish standardized protocols. For IoT security enhancement, both technological advancements and user education programs must be applied using a full-scale approach.

V. DISCUSSION

The results from this research bring essential knowledge that both academia and practitioners need to develop and apply cyber hygiene methods in IoT systems. This segment evaluates the study's outcomes through existing research literature before mentioning vital barriers while proposing development opportunities in this vital cybersecurity domain.

5.1 Addressing the Knowledge Gap in Cyber Hygiene

According to this research, users who operate IoT systems demonstrate substantial differences in knowledge understanding compared to experts in cybersecurity. The survey revealed that IoT users showed no knowledge of typical vulnerabilities affecting 65% while cybersecurity professionals displayed equal ignorance in the same area (Kaur et al., 2023; Rekha et al., 2023). The wide gap between the cybersecurity expertise of users and professionals requires immediate attention because it demands better programs for education and cybersecurity awareness centred on IoT devices. The available security initiatives currently neglect the protection requirements of everyday users because these users do not comprehend IoT device threats or available protection methods. The authors Baraković and

Baraković Husić (2023) emphasize that user education is a fundamental element to conquering security hurdles arising from poor password management and neglected system maintenance. Improving IoT security practices across the board will remain challenging because this critical deficiency is not being resolved.

5.2 The Role of Standardization and Regulation in IoT Security

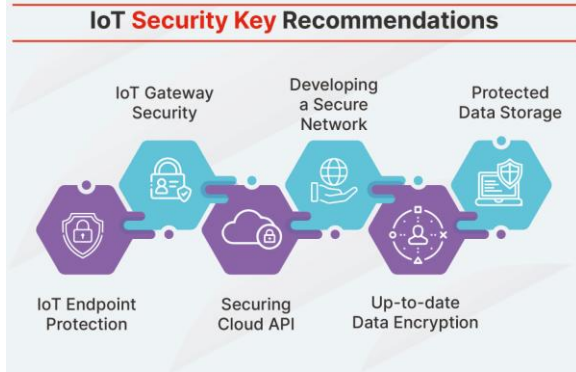


Figure 3: IoT Security Best Practices

One main challenge in this research centres around the inadequate standardization of protection methods for Internet of Things technology devices. The absence of standard security rules for IoT devices causes inconsistent security procedures, which leaves particular IoT devices unnecessarily exposed to attacks due to poorly configured systems and accessible software flaws. Olivares-Rojas et al. (2023) reported that experts described the troubles of implementing identical security policies throughout diverse IoT systems. The research outcome supports existing research that discusses the security difficulties that IoT creates due to its decentralized structure (Rekha et al., 2023). When manufacturers implement standardized security frameworks as traditional IT systems do, the number of existing vulnerabilities will decrease significantly. The major obstacle to IoT standardization exists because manufacturers remain fragmented from cybersecurity experts and regulatory bodies (Salem & Sobaih, 2023).

5.3 Behavioral Factors and User Compliance

User behavior is an essential factor that determines the security of IoT systems. Users continue to evade suggested security measures despite growing IoT security technology due to their resistance to following

cyber hygiene guidelines. Users who operate IoT devices fail to take basic security measures by using flimsy passwords and not installing updates, thus creating easy targets for cyber attacks (Chong et al., 2023). Much like Greuel et al. (2023) this research confirms that the best security enhancement method for IoT consists of technical solutions and user education initiatives. Security measures that include up-to-date features, robust authentications, and user-friendly security features help reduce safety risks stemming from user non-compliance. The security position of IoT systems requires all users to follow instructions regarding device setup protocols alongside multi-factor authentication usage to boost overall security readiness.

5.4 Implications for Policy and Industry Practices

Important guidelines from this analysis will substantially impact future policy and industrial operations. The development of IoT security regulations needs more attention because industry standards should enforce protected device implementation, scheduled software updates, and unhindered vulnerability reporting. Poor cyber hygiene practices will trigger increasing security challenges for IoT devices since these devices are increasingly vital to smart cities and industrial automation sectors' healthcare operations. Establishing secure design principles at the start of IoT systems development requires policymaking priority and industry collaboration. Efforts to standardize IoT devices should establish minimum security prerequisites, including secure boot systems, firmware verification mechanisms, and safe communication networks (Olivares-Rojas et al., 2023).

5.5 Future Research Directions

The research investigation identifies multiple directions academics can pursue in studying IoT security and cyber hygiene. Research should analyze the success of multiple educational methods to increase users' IoT security practice compliance. The security benefits of machine learning together with artificial intelligence for IoT protection need further assessment regarding their ability to deliver anomaly detection and real-time vulnerability management capabilities (Hore et al., 2023). Significant research gaps exist in understanding how industrial partnerships develop standardized security

frameworks and identify solutions to force regulatory agencies to make companies follow these standards. Time-based studies monitoring user conduct shifts and equipment protection developments throughout extended periods will create valuable information about educational and policy change effects.

CONCLUSION

The research emphasises the urgent need to enhance IoT cyber security practices by showing multiple critical discoveries in IoT security research development. Research findings reveal a substantial understanding of differences between regular IoT users and security experts, so establishing better education programs became vital for protecting against IoT vulnerabilities. Establishing universal security frameworks remains an ongoing challenge because of missing standardized security protocols for IoT devices. Therefore, manufacturers and regulatory bodies and cybersecurity experts must collaborate to develop these security frameworks.

The behavioural elements of IoT security require attention since users fail to follow security protocols even though technical solutions exist. User adoption of security measures in IoT devices depends heavily on the regular update cycle of devices, secure configuration setups, and user-friendly cybersecurity practices. The growing number of IoT devices throughout industries and everyday life makes strong security measures progressively crucial in safeguarding confidential information while stopping possible cyber-physical attacks.

IoT device manufacturers and policymakers must implement regulations that support secure design protocols while maintaining complete disclosure of vulnerabilities and device update information. Research results from this study enable further investigation about educational program effectiveness, emerging security technologies, and industrial protocols for standardization.

IoT cyber hygiene advancement requires multiple elements that combine knowledge programs with technology progressions and government regulations with user conduct modification initiatives. Security measures must be addressed now to protect the

steadily growing device networks, which are becoming the dominant force in modern digital systems.

REFERENCES

- [1] Alowais, S., Armeen, I., Sharma, P., & Johnston, A. (2023). Cyber hygiene practices across cultures: A cross-cultural study of us and saudi arabia based information systems users. In *Procedia Computer Science* (Vol. 219, pp. 744–750). Elsevier B.V. <https://doi.org/10.1016/j.procs.2023.01.347>
- [2] Al-Barakat, A. A., Al-Hassan, O. M., AlAli, R. M., Al-Hassan, M. M., & Al sharief, R. A. (2023). Role of female childhood education teachers in directing children towards effective use of smart devices. *Education and Information Technologies*, 28(6), 7065–7087. <https://doi.org/10.1007/s10639-022-11481-y>
- [3] Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioural practices of university students. *Information Security Journal*, 32(5), 347–370. <https://doi.org/10.1080/19393555.2022.2088428>
- [4] Basuki, A., & Adriansyah, A. (2023). Response time optimization for vulnerability management system by combining the benchmarking and scenario planning models. *International Journal of Electrical and Computer Engineering*, 13(1), 561–570. <https://doi.org/10.11591/ijece.v13i1.pp561-570>
- [5] Bunyitai, Á. (2023). Insider Threat Mitigation in High Security Facilities. *Nemzetbiztonsági Szemle*, 11(1), 49–61. <https://doi.org/10.32561/nasz.2023.1.4>
- [6] Cheng, L., & Cao, J. (2023). Factors influencing smart device addiction among preschool children: An extended protection-risk model perspective. *Frontiers in Psychology*, 14. <https://doi.org/10.3389/fpsyg.2023.1017772>
- [7] Compastié, M., López Martínez, A., Fernández, C., Gil Pérez, M., Tsarsitalidis, S., Xylouris, G., ... Šafran, V. (2023). PALANTIR: An NFV-Based Security-as-a-Service Approach for Automating Threat Mitigation. *Sensors*, 23(3). <https://doi.org/10.3390/s23031658>

- [8] Chong, J. L., Chew, K. W., Peter, A. P., Ting, H. Y., & Show, P. L. (2023). Internet of Things (IoT)-Based Environmental Monitoring and Control System for Home-Based Mushroom Cultivation. *Biosensors*, 13(1). <https://doi.org/10.3390/bios13010098>
- [9] Farghaly Abdelaliem, S. M., Dator, W. L. T., & Sankarapandian, C. (2023). The Relationship between Nursing Students' Smart Devices Addiction and Their Perception of Artificial Intelligence. *Healthcare (Switzerland)*, 11(1). <https://doi.org/10.3390/healthcare11010110>
- [10] Greuel, M., Sy, F., Bärnighausen, T., Adam, M., Vandormael, A., Gates, J., & Harling, G. (2023). Community Health Worker Use of Smart Devices for Health Promotion: Scoping Review. *JMIR MHealth and UHealth*. JMIR Publications Inc. <https://doi.org/10.2196/42023>
- [11] Guerrero-Ulloa, G., Rodríguez-Domínguez, C., & Hornos, M. J. (2023, January 1). Agile Methodologies Applied to the Development of Internet of Things (IoT)-Based Systems: A Review. *Sensors*. MDPI. <https://doi.org/10.3390/s23020790>
- [12] Hore, S., Shah, A., & Bastian, N. D. (2023). Deep VULMAN: A deep reinforcement learning-enabled cyber vulnerability management framework. *Expert Systems with Applications*, 221. <https://doi.org/10.1016/j.eswa.2023.119734>
- [13] Hemberg, E., Turner, M. J., Rutar, N., & O'Reilly, U. M. (2024). Enhancements to Threat, Vulnerability, and Mitigation Knowledge for Cyber Analytics, Hunting, and Simulations. *Digital Threats: Research and Practice*, 5(1). <https://doi.org/10.1145/3615668>
- [14] Ivanov, N., Li, C., Yan, Q., Sun, Z., Cao, Z., & Luo, X. (2023). Security Threat Mitigation for Smart Contracts: A Comprehensive Survey. *ACM Computing Surveys*, 55(14 S). <https://doi.org/10.1145/3593293>
- [15] Kaur, B., Dadkhah, S., Shooleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... Ghorbani, A. A. (2023, July 1). The evolution of Internet of Things (IoT) security dataset: Challenges and future directions. *Internet of Things (Netherlands)*. Elsevier B.V. <https://doi.org/10.1016/j.iot.2023.100780>
- [16] Kamerer, J. L., & McDermott, D. S. (2023). Cyber hygiene concepts for nursing education. *Nurse Education Today*, 130. <https://doi.org/10.1016/j.nedt.2023.105940>
- [17] Khurshid, K., Danish, A., Salim, M. U., Bayram, M., Ozbakkaloglu, T., & Mosaberpanah, M. A. (2023, January 1). An In-Depth Survey Demystifying the Internet of Things (IoT) in the Construction Industry: Unfolding New Dimensions. *Sustainability (Switzerland)*. MDPI. <https://doi.org/10.3390/su15021275>
- [18] Lin, J., Zhang, H., Adams, B., & Hassan, A. E. (2023). Vulnerability management in Linux distributions: An empirical study on Debian and Fedora. *Empirical Software Engineering*, 28(2). <https://doi.org/10.1007/s10664-022-10267-7>
- [19] Machireddy, Jeshwanth, Harnessing AI and Data Analytics for Smarter Healthcare Solutions (January 14, 2023). *International Journal of Science and Research Archive*, 2023, 08(02), 785-798, Available at <http://dx.doi.org/10.2139/ssrn.5159750>
- [20] Moslehi, S., Dehghani, A., Masoumi, G., & Barghi Shirazi, F. (2023). Vulnerability Management of the Elderly During COVID-19 Pandemic: A Systematic Review. *Health in Emergencies and Disasters Quarterly*, 8(2), 77–86. <https://doi.org/10.32598/hdq.8.2.310.3>
- [21] Maleh, Y., Qasmaoui, Y., El Gholami, K., Sadqi, Y., & Mounir, S. (2023, June 1). A comprehensive survey on SDN security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments*. Springer Science and Business Media Deutschland GmbH. <https://doi.org/10.1007/s40860-022-00171-8>
- [22] Machireddy, Jeshwanth, Automation in Healthcare Claims Processing: Enhancing Efficiency and Accuracy (April 16, 2023). *International Journal of Science and Research Archive*, 2023, 09(01), 825-834, Available at <http://dx.doi.org/10.2139/ssrn.5159747>
- [23] Mostofa, K. Z., & Islam, M. A. (2023). Creation of an Internet of Things (IoT) system for the live

- and remote monitoring of solar photovoltaic facilities. *Energy Reports*, 9, 422–427. <https://doi.org/10.1016/j.egy.2023.09.060>
- [24] Mundt, M., & Baier, H. (2023). Threat-Based Simulation of Data Exfiltration Toward Mitigating Multiple Ransomware Extortions. *Digital Threats: Research and Practice*, 4(4). <https://doi.org/10.1145/3568993>
- [25] Olafuyi, B. A. (2023). Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation. *International Journal of Scientific and Research Publications*, 13(12), 194–200. <https://doi.org/10.29322/ijsrp.13.12.2023.p14419>
- [26] Olivares-Rojas, J. C., Reyes-Archundia, E., Gutiérrez-Gnecchi, J. A., Molina-Moreno, I., Méndez-Patiño, A., & Cerda-Jacobo, J. (2023). Cyber Hygiene in Smart Metering Systems. *Computacion y Sistemas*, 27(2), 459–475. <https://doi.org/10.13053/CyS-27-2-3894>
- [27] Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, 80, 3554–3559. <https://doi.org/10.1016/j.matpr.2021.07.295>
- [28] Salem, M. A., & Sobaih, A. E. E. (2023). A Quadruple “E” Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic. *Electronics (Switzerland)*, 12(10). <https://doi.org/10.3390/electronics12102268>
- [29] Tsang, H., Salahuddin, M. A., Limam, N., & Boutaba, R. (2023). Meta-ATMoS+: A Meta-Reinforcement Learning Framework for Threat Mitigation in Software-Defined Networks. In *Proceedings - Conference on Local Computer Networks, LCN*. IEEE Computer Society. <https://doi.org/10.1109/LCN58197.2023.10223403>
- [30] Wenzel, M., Rowland, Z., Nielsen, K. S., & Lange, F. (2023). Too much praise for reappraisal? Examining reappraisal’s impact on threat mitigation depending on its implementation: A registered report. *Journal of Experimental Social Psychology*, 107. <https://doi.org/10.1016/j.jesp.2023.104475>
- [31] Yan, W., & Ji, S. (2023). A secure and efficient DSSE scheme with constant storage costs in smart devices. *Cyber Security and Applications*, 1. <https://doi.org/10.1016/j.csa.2022.100006>
- [32] Yemshanov, D., Dawe, D. A., Bakalarczyk, A., Liu, N., Boulanger, Y., Boucher, J., ... Parisien, M. A. (2023). Balancing wildlife protection and wildfire threat mitigation using a network optimization approach. *Frontiers in Forests and Global Change*, 6. <https://doi.org/10.3389/ffgc.2023.1186616>