SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

A Comparative Framework for IoT Cyber-Attack Mitigation Strategies During the COVID-19 Era: A Deep Analysis of Vulnerabilities, Countermeasures, and Real-World Applicability

Ackmez Allamammaly

IT Analyst, Department of Information Technology, Mauritius Institute of Education (MIE), Reduit, Mauritius.
E-mail: a.ackmez@mie.ac.mu, ORCID: 0009-0004-8230-8603

ABSTRACT
The COVID-19 epidemic expedited worldwide dependence on Internet of Things (IoT) technology in healthcare, education, enterprise systems, and public services, which resulted in rapid deployment of unscheduled technology solutions. The exceptional growth of IoT devices generated serious security threats that originated from multiple device environments, poor basic security settings, limited device processing capacity, and unprotected residential Wi-Fi connections. IoT systems experienced a drastic rise in cyber threats which included phishing attacks, ransomware attacks, DDoS attacks, spoofing attacks, and unauthorized access attempts. The current research provides taxonomies and systematic evaluations, but there needs to be more structured studies that compare different mitigation methods for emergency operational settings. This paper establishes a multi-criteria comparative framework to evaluate IoT cyber-attack mitigation solutions which assess effectiveness and scalability and resource overhead and crisis feasibility and cross-sector applicability. The paper uses SLR-based thesis dataset insights and pandemic-era case scenarios to evaluate VPNs and MFA and secure routing protocols and ML-based intrusion detection and blockchain authentication and encryption techniques and human-centric controls. The research results show that secure routing and VPN and MFA network-layer methods provide the strongest security protection, while resource-constrained IoT devices should use lightweight encryption together with secure protocols. Blockchain and machine learning methods can provide strong security solutions, yet they face difficulties when used in emergency situations. The recommended comparison framework provides politicians and healthcare professionals and organizations and IoT platform developers with effective guidance to choose appropriate mitigation solutions through their analysis of current and upcoming crisis situations.

Keywords: IoT Security; COVID-19 Cybersecurity; Cyber-Attack Mitigation; Comparative Framework

Introduction

The covid-19 pandemic resulted in digital transformation which increased worldwide dependence on Internet of Things (IoT) technologies because of rapid technological advancements. The organizations started to implement remote work policies while healthcare systems expanded their telemedicine services and educational institutions adopted online and hybrid learning models and governments deployed smart monitoring devices to monitor their citizens and IoT devices became available as operational continuity solutions (Shanmuganathan and Mahendran, 2021). This wave was unprecedented and resulted in mass and in many cases unplanned IoT implementation in industries, including transportation, healthcare, retail, entertainment, and education and communication as seen in figure 1. Nevertheless, this rapid adoption also came with serious cybersecurity issues, most of which were increased due to the neediness and magnitude of the growth of IoT in the pandemic times. The paper mentions that often, the deployed devices lacked standard security settings, firmware, or the appropriate method of inclusion, and thus, they were extremely susceptible to abuse (Munmun and Paul, 2021). The cyber vulnerability was also enhanced by the heterogeneity of IoT ecosystems, limited computational capacity, and poor inbuilt security capabilities (Shammari et al., 2021}.

Figure 1. Application of IoT during the COVID-19 pandemic (Yousif et al., 2021).

The COVID-19 period showed a significant rise in cybersecurity attacks against IoT systems which included malware infections DDoS attacks ransomware attacks phishing-based intrusions and data theft incidents according to research conducted by Khokhar and his colleagues in 2024. The pandemic resulted in a major increase of vulnerabilities found within IoT systems. The criminals took advantage of the different access points that were made available due to remote work, home networks that were not secured, and IoT devices that were not well protected at all. The incidents called for the necessity of robust, mobile, and specific to the situation mitigation strategies to protect health-care IoT systems under crisis conditions, thereby creating a very obvious reasoning for the inquiry into the various security measures' effectiveness and practicality (Siwakoti et al., 2023).

The rapid growth of IoT ecosystems caused by the pandemic led to the occurrence of cyber-attacks on an unprecedented scale and consequently resulted in multiple studies being conducted—taxonomies, SLRs, and descriptive analyses—but most of them only pinpointed weaknesses and provided a list of solutions without thoroughly assessing their practical performance in a systematic way. This situation indicates the need for a full-fledged comparative framework that would facilitate the evaluation of the measures that are possible, scalable, and effective that would be compatible with the IoT deployments in pandemic times and in the future saleous et al., 2023).

In line with that, the current study aims to establish a framework that compares different e-commerce cybersecurity measures against cyber-attacks based on the three criteria of effectiveness, scalability, and performance, thus providing an action-oriented model to help stakeholders choose the right security measures for real-world application.

The comparative framework is particularly useful in:

1. Government agencies, assisting in the formation of cybersecurity policy in the state of crisis circumstances;
2. Healthcare systems, where the increased dependencies on IoT and cyber-risks were experienced during COVID-19;
3. Remote-work and enterprise system, that needs robust and deployable IoT security solutions;
4. IoT platform developers and solution providers, who require a systematic approach to setting priorities in mitigating heterogeneous device ecosystems.

This study provides an empirically based, multi-criteria evaluation tool that improves readiness for potential large-scale disruptions and adds innovative methodological value to IoT cybersecurity research.

Literature Review

Andrade et al. (2020) found that COVID-19 changed the way cybersecurity worked a lot because businesses moved their work from cities to remote telework environments. Residential cybersecurity architecture did not have the same level of protection as businesses, especially when the home had smart infrastructure,

which made it easier for hackers to get in. This setting helped the number of attacks go up a lot, by more than 35%. VPN solutions were used to protect communications while working from home, but security attacks took advantage of weaknesses in home equipment and people, making VPN solutions less effective. The attackers focused on social engineering attacks that took advantage of people's fears about the COVID-19 pandemic to make their attacks more effective. This study examined cybersecurity attacks that arose during the pandemic and the subsequent need to adapt protective measures in cybersecurity.

According to the study by Susukailo et al. (2020), social engineering was the most prevalent form of cyber-attack during the COVID-19 pandemic. The various techniques of social engineering attacks were exhibited. Also, the Zoom app was used to show how cyber attacks work. The discussions included various methods to prevent cyberattacks which included remote security management and monitoring and BCM and cybersecurity awareness training and the enhancement of device and service security. Wang and Alexander's (2021) study showed that COVID-19 changed how businesses around the world thought about cybersecurity. Home-based work became necessary for many employees during the COVID-19 pandemic who used their personal computers and routers and antivirus software for work purposes. People established cybersecurity measures to protect themselves from hacking attempts but those measures failed to safeguard their most sensitive data. This paper delineated significant technologies, including 5G, blockchain, telemedicine, and big data, that were employed in combating COVID-19, cyber-attacks, and cyber risks arising from human actions and technological failures during the pandemic. Among the topics discussed were cyber security for remote work, Internet of Things (IoT), telemedicine and cyber security powered by blockchain. Blockchain technology ensured that the medical sector was more secure, less privacy-invasive, and posed less risk in the spread of COVID-19. Mondal and Mitra (2022) announced the epidemic's revolutionary effects on the world's systems and pointed out that it pushed technology's acceptance further. Their research proved that IoT and AI were the pillars of the pandemic management through real-time monitoring, tracking, and response across healthcare, economy, and education sectors. Although there are numerous studies regarding the use of IoT during the pandemic, Mondal and Mitra pointed out that the primary design problems-white, kiki, and the like—are still under-researched. Based on their review of the literature, IoT was the major factor that impeded the crisis management process and ushered in the "new normal," with the accentuation of the prevailing difficulties and the requirement for a more robust integration in the post-pandemic era.

Artificial Intelligence has been considered as an option for cybersecurity among other solutions. Macas et al. (2022) Lezzi et al., (2025) noted that ML is increasingly used across sectors, particularly within IoT, to strengthen security. ML helps protect IoT devices and networks from attacks and detects anomalies using algorithmic pattern analysis. In the study Al-qahtani and Cresci,(2022) The percentage of several techniques for cyber-attacks during the COVID-19 pandemic were provided. Cyber-attacks were mostly phishing attacks. The different phishing attacks and their mitigation techniques were provided.

The literature reviewed demonstrates that the COVID-19 changed the landscape of cybersecurity around the world considerably, revealing the new vulnerabilities of remote-work systems, IoT devices, and even virtual services. Specific threats, which include social engineering (Andrade et al., 2020; Susukailo et al., 2020), telework-related insecurity (Wang and Alexander, 2021), and challenges with the adoption of IoT technologies (Mondal and Mitra, 2022) by other researchers in the field were identified and the subsequent rise in the use of AI/ML and blockchain technologies to improve cybersecurity was analyzed (Macas et al., 2022; Al-qahtani and Cresci, 2022)

One of the main novelties of the work is its ability to combine the IoT vulnerabilities of the numerous layers with the corresponding mitigation measures, which allows mapping this aspect in a systematic way which had not been investigated in the context of pandemic-related cybersecurity studies. Also, the research includes cross-sector contextualization, in which mitigation strategies are not just in the area of healthcare IoT but also in remote-work, smart education, logistics, and other urgent areas of the pandemic.

Research Methodology

The paper describes the methodological framework that is used to create a comparative analysis of the strategies of mitigating IoT cyber-attacks in the period of the COVID-19. Because the investigation builds upon the SLR-based taxonomy. This paper brings in an aspect of comparison considering that there are evaluation parameters are brought in, including real-world applicability, performance effectiveness, constraints of deploying the layer during a crisis setting, layer vulnerabilities that are specific to its application, and cross-sector flexibility.

Research Design

This research study is a hybrid qualitative-quantitative comparative study.

The qualitative aspect integrates the weaknesses and countermeasures measures, grounded on proven secondary sources, such as the SLR result, that identified the attacks and countermeasures across the various IoT layers during the COVID-19. Its quantitative part uses a structured multi-criteria evaluation

model to rank and compare mitigation plans with COVID-related operational limitations to facilitate the research go beyond willingly descriptive taxonomies and generate a quantifiable, decision-oriented comparative model.

Data Input
The framework is developed from secondary data, which encompasses:

IoT Vulnerabilities
An overview of the layer-wise threats, i.e., DoS, MITM, spoofing, side-channel attacks, ransomware, and malware campaigns, that were intensified throughout the pandemic.

Mitigation Techniques
SLR and taxonomy of mitigation strategies, such as ML-based IDS, authentication protocols (MFA, CBA), secure routing (RPL, AMQP), VPN, encryption mechanisms, policy-based controls, and awareness-based countermeasures.

COVID-19 Contextual Data
The operational limitations, industry-specific issues, and the patterns of attacks (e.g., exploitation of IoT in healthcare, the vulnerability of WFH devices, Zoom-raiding, phishing boom) are intertwined into the comparison model as weighting factors.

Framework Construction Approach
Step 1: Determine Evaluation Standards.
The criteria are based on the realities of the pandemic period of operations like remote access, heterogeneous devices, network congestion, the use of old hardware, phishing, and pressure on the healthcare system.
The decision criterion will be the final assessment:
1. Effectiveness (Attack Resistance Strength): Capacity to mitigate, eliminate, or identify cyber-attacks on the layers of the IoT.
2. Scalability: Applicability to large scale deployments (e.g., mass WFH, healthcare IoT deployments).
3. Resource Overhead: CPU, memory, bandwidth, and power consumption - vital because of the resource-starved IoT devices.
4. Deployment Feasibility: The facility to integrate easily in case of an emergency situation; the capability to align with an older IoT infrastructure.
5. Applicability in the Real Life: Confirmed efficacy in real-life situations of COVID-19 (e.g., telemedicine, distance education systems).
6. Layer-Coverage Breadth: In relation to the multi-layered models, whether the strategy secures one or more layers of IoT (perception towards business) or not.

Step 2: Multi-Criteria Decision Modelling
A weighted scoring system, inspired by Analytical Hierarchy Process (AHP), is used to:
1. Assign weights to each criterion based on relevance during COVID-19 (e.g., applicability and scalability receive higher weight due to pandemic constraints).
2. Score each mitigation strategy
3. Compute a composite score for each strategy using a normalised weighted average.

This allows objective comparison of strategies such as MFA, VPN, ML-based anomaly detection, blockchain-enabled integrity, protocol-level security, and network segmentation.

Validation Strategy
The concept is validated by real-world scenarios from the COVID-19 era:
1. Attacks on Healthcare IoT Systems: Utilization of hospital IoT devices, medical sensors, and remote monitoring instruments.
2. Exploits in Video Conferencing (e.g., Zoom Raiding): Increase in social engineering and virus assaults via digital platforms utilized in education and commerce.
3. Compromises in Smart-City COVID Surveillance Systems: Risks to intelligent monitoring devices, unmanned aerial vehicles, thermal imaging systems, and contact-tracing technologies.
4. Remote Work Infrastructure Attacks: Exploitation of unmonitored routers, obsolete IoT devices, vulnerable Wi-Fi configurations, and cloud misappropriation.

Result Analysis

A comparative examination of IoT vulnerabilities, cyber-attack patterns, and mitigation strategies during the COVID-19 pandemic as seen in figure 2 and 3. The comparative matrix looks at three things when comparing key mitigation strategies: how well they work in layers, how well they work when there are problems caused by the pandemic (like limited bandwidth, difficulty updating from afar, and low-trust home networks), and how well they can be used in real life. The study shows that network-layer methods like safe routing (RPL), VPN installation, multi-factor authentication (MFA), and encryption provide the best basic security, especially in times of crisis. Application-layer techniques, such as firewalls, secure authentication systems, and anti-phishing measures, proved highly effective against the rise in application-level threats like credential theft and ransomware during the pandemic. On the other hand, perception-layer methods like firmware management and hardware hardening were limited by supply chain problems and the fact that maintenance couldn't be done on-site during lockdowns. Strong technologies like machine learning-based intrusion detection and blockchain technology showed a lot of promise in theory, but they ran into problems when it came to putting them into practice because of bandwidth limits, processing needs, and problems with remote maintenance.

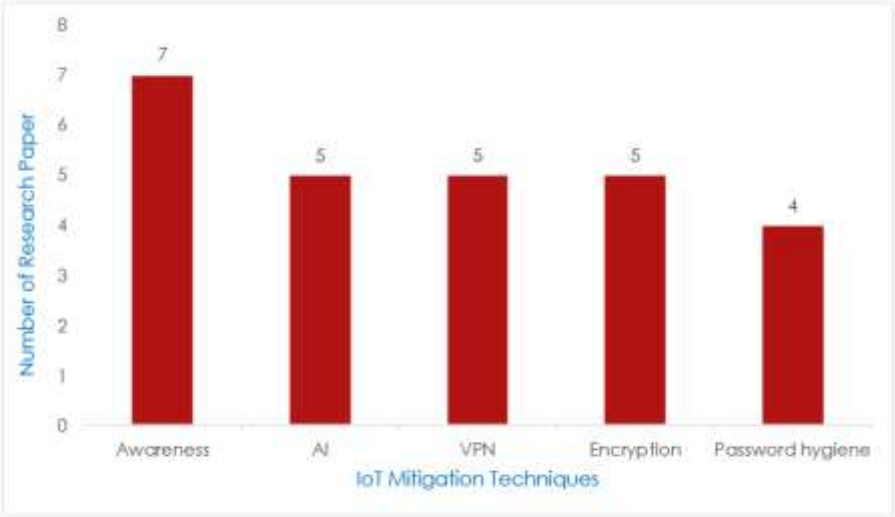

Figure 2. Top five IoT mitigation techniques during COVID-19.

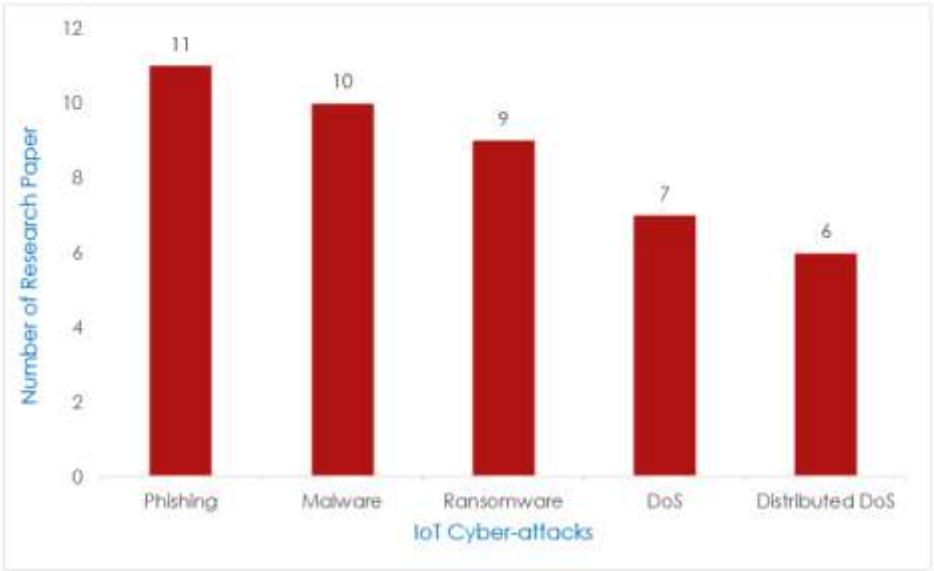

Figure 3. Top five common IoT cyber-attacks during COVID-19.

The framework used multi-criteria scoring to assess mitigation solutions according to their complete effectiveness and operational efficiency and their ability to function in different Internet of Things (IoT) environments. The combination of secure routing with multi-factor authentication and virtual private networks plus updated firmware security systems delivered complete protection through all Internet of Things (IoT) security levels while enabling operators to implement instant security measures during the

pandemic. The testing showed that lightweight encryption and secure protocols (AMQP, CoAP-DTLS, IEEE 802.15.4) delivered their highest performance in resource-limited Internet of Things (IoT) systems which included small sensors and wearable health devices and low-power industrial nodes. The figure 4 indicates the IoT categories during COVID 19 and that includes cyber-attack as well as mitigation technique. The combination of blockchain-based authentication systems and IDS/IPS monitoring systems created better trust and system integrity and improved traceability for telemedicine and electronic health records (EHR) and remote patient monitoring in healthcare environments. On a national level, cloud-based data aggregation coupled with centralized VPN designs demonstrated optimal effectiveness for extensive COVID-19 tracking and coordination initiatives because to their scalability and centralized management.

Figure 4. Taxonomy of IoT cyber-attacks during COVID-19 and mitigation techniques.

Several critical insights arose from the comparison findings. Theoretical use of many advanced solutions was restricted to the extent of pandemic constraints, because deep learning IDS and blockchain systems were too resource-heavy for quick deployment. The research demonstrated that human-focused

educational programs together with public awareness initiatives and compliance measures represented the most economical solution to protect against phishing threats which made up almost 33 percent of the total security incidents. Emergency situations needed urgent solutions because blockchain technology offered trust and unchangeable records but its speed did not meet emergency response requirements. The network layer security system provided organizations with the best combination of security features because it delivered both extensive protection and practical operational benefits.

Discussion

This review analysed the IoT cyber-attacks that occurred during the pandemic, revealing the various defensive measures taken, and discussed the pros and cons of each measure along with their impacts. It basically scrutinized if a taxonomy could be associated with 3-layered or 4-layered IoT models and if certain attacks could be linked to appropriate defences. The research, however, indicated otherwise: thirteen attacks had no known mitigation, and twenty-two and twenty-three attacks could not be correlated with the 3-layered and 4-layered architectures, respectively. It was ultimately determined that constructing a taxonomy of IoT mitigation techniques using either the 3-layered or even the 4-layered IoT architecture models was impractical. Per the conclusions of the current SLR, twenty-one IoT mitigation techniques could not be classified within the layers of the 3-layered architecture, while twenty techniques did not fit within the layers of the 4-layered architecture.

Conclusion

The research provides a comparison between the IoT cybersecurity protocols that were adapted in the course of the pandemic. It reveals that the most effective in the fight against IoT security were measures applied at the network layer (secure routing, MFA, updates, VPNs) and tools at the application layer (anti-phishing, strong authentication). ML-based detection and blockchain were demonstrating their potentials but did not reach the full deployment stage. The entire research interprets that security for IoT devices necessitates the application of both, strong technical defenses, and user-centric measures, thus accumulating the need for adaptive and real-time security models to facilitate the developing of IoT ecosystems that are more resilient and ready for crises.

References

1. Shammari, A.A., Maiti, R.R. and Hammer, B. (Mar 10, 2021) Organizational Security Policy and Management during Covid-19. IEEE, pp. 1.
2. Shanmuganathan, H. and Mahendran, A. (Sep 24, 2021) Current Trend of IoT Market and its Security Threats. Piscataway: IEEE, pp. 1.
3. Khokhar, R. H., Rankothge, W., Rashidi, L., Mohammadian, H., Ghorbani, A., Frei, B., Ellis, S., & Freitas, I. (2024). A survey on supply chain management: Exploring physical and cyber security challenges, threats, critical applications, and innovative technologies. International Journal of Supply and Operations Management, 11, 250–283.
4. Siwakoti, Y.R., Bhurtel, M., Rawat, D.B., Oest, A. and Johnson, R. (2023) 'Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks and Countermeasures', IEEE internet of things journal, , pp. 1 Available at: 10.1109/JIOT.2023.3252594.
5. Saleous, H., Ismail, M., AlDaajeh, S.H., Madathil, N., Alrabaee, S., Choo, K.R. and Al-Qirim, N. (2023) 'COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities', Digital Communications and Networks, 9(1), pp. 211-222 Available at: 10.1016/j.dcan.2022.06.005.
6. Munmun, F.A. and Paul, M. (Aug 05, 2021) Challenges of DDoS Attack Mitigation in IoT Devices by Software Defined Networking (SDN). Piscataway: IEEE, pp. 1.
7. Wang, L., & Alexander, C. Cyber security during the COVID-19 pandemic. . 2021; 5.
8. Andrade, R., Ortiz-Garcés, I., & Cazares, M. Cybersecurity Attacks on Smart Home During Covid-19 Pandemic. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). 2020.
9. Mondal, S., & Mitra, P. The Role of Emerging Technologies to Fight Against COVID-19 Pandemic: An Exploratory Review. Transactions of the Indian National Academy of Engineering. 2022; 7.
10. Susukailo, V., Opirskyy, I. and Vasylyshyn, S. (Sep 23, 2020) Analysis of the attack vectors used by threat actors during the pandemic. IEEE, pp. 261.
11. Macas, M., Wu, C. and Fuertes, W. (2022) 'A survey on deep learning for cybersecurity: Progress, challenges, and opportunities', Computer networks (Amsterdam, Netherlands: 1999), 212, pp. 109032 Available at: 10.1016/j.comnet.2022.109032.
12. Al-qahtani, A.F. and Cresci, S. (2022) The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19 Institution of Engineering and Technology (IET).

13. Yousif, M., Hewage, C. and Nawaf, L. (2021) 'IoT Technologies during and Beyond COVID-19: A Comprehensive Review', Future internet, 13(5), pp. 105 Available at: 10.3390/fi13050105.
14. Lezzi, M., Montefusco, P., Lazoi, M., & Corallo, A. (2025). AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions. Journal of Industrial Information Integration, 48, 100980.