SYM-AM-26-130

Excerpt from the Proceedings

of the

Twenty-Third Annual Acquisition Research Symposium and Innovation Summit

Volume III

"Accelerating Warfighting Capabilities"

IoMT Cybersecurity:
A Systems Perspective

Published: April 30, 2026

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

The research presented in this report was supported by the Acquisition Research Program, Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, please contact:

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
E: arp@nps.edu
www.acquisitionresearch.net

Copies of Symposium Proceedings and Presentations; and Acquisition Sponsored Faculty and Student Research Reports and Posters may be printed from the **NPS Defense Acquisition & Innovation Repository** at **https://dair.nps.edu/**.

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF ACQUISITION, FINANCE, AND MANPOWER
NAVAL POSTGRADUATE SCHOOL

IoMT Cybersecurity: A Systems Perspective

Babajide Asaju—IoMT Cybersecurity A Systems Perspective, Naval Postgraduate School. [basaju@npsfoundation.org]

Abstract

The rapid expansion of Internet connected devices and cyber physical systems has undoubtedly increased the complexity of modern cybersecurity environments. Internet of Things (IoT) ecosystems, particularly those involving Internet of Medical Things (IoMT) devices introduce heterogeneous architectures that expand the attack surface and expose systems to distributed denial of service (DDoS) attacks, spoofing, and network intrusion. Traditional security models often concentrate on isolated vulnerabilities rather than the systemic interactions that allow attacks to proliferate across interconnected infrastructures. This study delves into cybersecurity vulnerabilities from a systems perspective by analyzing attack behaviors across Wi-Fi enabled IoMT devices and simulated MQTT environments. Network traffic was captured using controlled laboratory experiments and analyzed through packet capture PCAP datasets to identify patterns of DDoS reconnaissance and spoofing attacks. The results highlight how device-level weaknesses, such as weak authentication and unpatched firmware, interact with network-level vulnerabilities including poor segmentation and insecure protocols to amplify systemic cyber risk. The study contributes to classification of IoT and cyber physical system vulnerabilities and provides defensive mitigation strategies including identity management cryptographic controls network segmentation and continuous risk assessment for complex IoT environments. These discoveries provide insights into securing cybersecurity architecture across smart infrastructures of both healthcare systems and critical cyber physical environments.

Keywords: DDoS attack, vulnerability, cybersecurity, cyber physical systems, IoT, IoMT

Introduction

The rapid integration of digital technologies into modern infrastructure has significantly expanded the importance and complexity of cybersecurity challenges when it comes to addressing common security issues. Contemporary cyber ecosystems now consist of highly interconnected devices networks and services that operate across heterogeneous environments. These environments involve cloud platforms, edge devices, Internet of Things (IoT) networks, and cyber physical systems (CPS) that support critical applications in healthcare transportation energy and smart city infrastructure. While these systems provide operational efficiency and technological advancement, they also introduce complex cybersecurity vulnerabilities that adversaries can exploit. Cybersecurity vulnerabilities are no longer limited to individual software flaws or isolated network misconfigurations. Instead, vulnerabilities increasingly emerge from the interaction between devices communication protocols software dependencies and operational environments. As interconnected systems grow in complexity the attack surface expands, and adversaries can exploit systemic weaknesses that propagate across multiple layers of cyber infrastructure (Mallick et al., 2024).

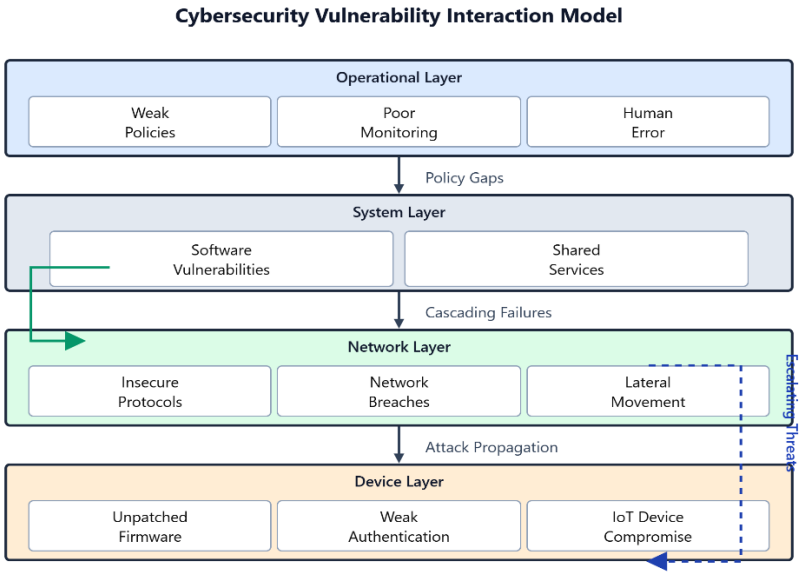


Figure 1. Multi-layer Cybersecurity Vulnerability Interaction Model

Figure 1, Multi-layer Cybersecurity Vulnerability Interaction Models, shows how vulnerabilities travel across network devices, and operational layers in Internet of Medical Things (IoMT) and cyber-physical environments. However, this growing complexity has led scholars to examine key components of cybersecurity vulnerabilities, particularly through systems findings that study how diverse forms of technological components communicate to minimize emergent security risks (Nukpezah, 2020; Özcan, 2026). IoT ecosystems and cyber physical systems continue to uncover new forms of security challenges that traditional models struggle to address.

These systems combine physical procedures with embedded computation and network communication, which creates tightly coupled dependencies between digital and physical environments. According to the research conducted by Kouloumpris (2026), CPSs and IoT systems must be designed and operated under a unified view of safety and security characteristics because the deal with the physical world. Understanding the systemic nature of these vulnerabilities is therefore essential for developing effective cybersecurity strategies (Motlagh, 2026).

This study investigates cybersecurity vulnerabilities from a systems perspective particularly on IoT software and cyber-physical environments. By investigating behavioral attacks on targeted Wi-Fi enabled IoMT devices and MQTT communication environments, the study analyzes how devices, through network levels, can be exposed to system level dependencies that can contribute to cybersecurity risks in complex infrastructures.

This study examines cybersecurity vulnerabilities from a systems perspective by addressing three core dimensions. First, it analyzes the architectural and operational factors that contribute to vulnerabilities in IoT and cyber physical systems. Second, it investigates how interactions between device level and network level weaknesses enable large scale cyber-attacks such as denial of service and distributed denial of service attacks. Third, it evaluates defensive strategies capable of mitigating systemic vulnerabilities in interconnected IoT environments.

Statement of the Problem

Despite several studies conducted in cybersecurity, existing studies still focus primarily on isolated vulnerabilities such as software flaws or configuration errors. While these approaches typically provide valuable insights, they often fail to account for the systemic nature of vulnerabilities that emerge within interconnected cyber ecosystems. Modern infrastructures, including IoT environments and cyber physical systems, consist of heterogeneous devices, communication protocols, and distributed computing architectures that interact in complex ways (Pundir et al., 2022). A single flaw can spread and cause a massive security disaster. As IoT devices and cyber-physical systems focus on expansions across critical infrastructure such as smart homes infrastructures and industrial networks, the potential impact of systemic vulnerabilities will continue to increase. Understanding how vulnerabilities emerge interact and propagate across complex systems is therefore essential for improving cybersecurity resilience and protecting critical infrastructure (Olasehinde et al., 2026).

Literature Review

Contemporary research necessitates the swift expansion of digital infrastructures capable of revolutionizing the management, storage, and processing of networks. Although numerous technological advancements have facilitated the integration of automation, they have concurrently introduced complex challenges within interconnected systems. As digital ecosystems grow in scale and complexity, it is imperative to identify effective strategies for mitigating vulnerabilities, thereby addressing significant gaps in the literature concerning integrated cybersecurity frameworks capable of managing systemic risks (Mokhonoana, 2026).

Arquilla and Ronfeldt (1993) characterized cyberwar as the disruption or destruction of information and communication systems through strategic digital attacks, emphasizing the strategic significance of networked systems in modern security contexts. As cyber-physical systems become increasingly embedded in critical sectors such as healthcare, transportation, and smart home environments, the imperative to secure these integrated infrastructures has intensified. Cyber-physical systems integrate computation, networking, and physical processes, implying that vulnerabilities in digital components can extend into real-world systems (Vidyalakshmi, 2025). The advent of the IoMT further exacerbates these concerns, as connected medical devices introduce substantial security and privacy vulnerabilities, necessitating enhanced risk assessment and protection mechanisms to safeguard healthcare infrastructures (Nithyavani, 2025).

The historical evolution of cybersecurity research can be traced to early cyber incidents that exposed weaknesses in networked environments. A notable example is the Morris Worm of 1988, which demonstrated how a single malicious program could rapidly propagate across the nascent Internet, disrupting extensive portions of network infrastructure (Raman, 2025). This incident underscored the necessity for stronger defensive mechanisms and marked a pivotal moment in cybersecurity research. Subsequent studies have highlighted that vulnerabilities frequently stem from flaws in system design, software implementation, and human interaction with technology (Molade, 2025; Verma, 2025). These incidents underscore the ongoing challenge of securing increasingly complex technological systems and reinforce the necessity for more robust cybersecurity frameworks capable of protecting critical infrastructure.

Cybersecurity Vulnerability

Understanding security is crucial from the perspective of intrusion and can also be understood as protecting against undesirable disclosure, destruction, or modification of data in a system, as well as the protection of the systems themselves. According to research conducted by ISACA, cybersecurity is concerned with the security and privacy of digital assets-everything

from networks to computing devices and information that is processed, stored, or exchanged by working information systems of the Internet (Sharma & Shambharker, 2025).

Through the concept of the International Telecommunications Union, cyber security is described as the collation of policies, techniques, and rules of institutional practice establishments used to protect the cyber assets of users within an organization. Computer security encompasses the protection of systems and data from unauthorized penetration, which is achieved through cybersecurity techniques and access control mechanisms (Vidović, 2025).

IoT Security Vulnerability

Much research has been conducted on the aspects of CPS and IoT to prototype system security, which is vital for addressing concerns. First, IoT is an extension of the Internet which means that IoT can coexist with different functionalities of networks among the interoperability for the delivery of various applications. Alfahaid et al. (2025) discussed IoT security vulnerabilities and challenges, including applications, networks, and physical systems. Their analysis covered security and privacy issues in diverse technologies (Alafahaid et al., 2025). Interconnectivity is vital for addressing the architectural problems of IoT. In addition to the previously mentioned challenges and opportunities in IoT besides the survey papers.

CPS Security Environment

CPS are integrations of combined units of physical procedures, including networking and computation. After a series of experiments, Vidyalakshmi et al. (2025) and Dias et al. (2025) concluded that the physical process is monitored and controlled by embedded (cyber) subsystems through networked systems with feedback loops to change their behavior when required (Dias et al., 2026). Most of these subsystems can operate independently of each other with the ability to communicate with the external environment. However, this type of communication requires different sensing devices to be processed without obstacles.

CPS Security Analysis

Similarly to many technical security challenges, computer security systems integrate both physical and cyber architectures (Damianou, 2025). Several security probabilities must be put into place when constructing to put together the designed mechanisms, as the landscape for forward thinking changes is constantly revolving with several challenges to address that are highly dynamic. Various risks constantly threaten the field of CPS, as emphasized by the National Institute of Standards and Technology (NIST). To address these risks and ensure the security of CPS, it is essential to implement a meticulously designed risk assessment. This assessment will not only provide an overall view of the security status of CPS but also allow for the efficient allocation of safeguard resources (Aljumaiah et al., 2025).

Related Work

The cyber environment encompasses a wide range of scholarly studies and literature. It should be mentioned that a sizable portion of these studies did not directly address the challenges posed by cybersecurity vulnerabilities, which have the potential to endanger infrastructure (Achuthan et al., n.d.) In the following lines of study, we will explore research that specifically addresses these issues and sheds light on the importance of cyber security.

In a comprehensive investigation that was conducted, the authors focused on mapping physical systems to cybersecurity in this study. Several reviews included domains such as network systems, automatic control, information systems, and smart grids. In smart grid domains, it is interesting to observe that many studies primarily emphasize physical-level attacks. Conducted an SLR on private adaptations for CPS (Moriano, 2025).

The primary objective was to refine their findings by examining the current approach used to address self-adaptation concerns in later communications between CPSs, where existing solutions incorporate a combination of adaptation mechanisms across different layers. Therefore, further research is required to investigate the mapping of solutions between different layers of self-adaptation in CPS. Edrisi (2025) studied smart grid and SCADA security solutions for existing cyberattacks. This study focuses on the current state of cyberattack security architecture to model the consequences of these attacks and their detection methods.

IOT and CPS Vulnerabilities: Drivers, Classes, and Mitigation Strategies

Overview and Why Vulnerabilities Are Rising

The rapid progression of interconnected medical devices within the IoT has increasingly moved the attack surface of CPS and critical infrastructure. Many IoT devices are inherently resource deprived, with limited processing power, memory, and battery size, reducing the use of effective cryptographic protocols, secure authentication, and numerous patches (Damianou, 2025).

Furthermore, IoT ecosystems are highly heterogeneous and incorporate distinct firmware, communication protocols, security standards, and updating practices. This heterogeneity, which is related to the lack of global standardization, leads to illogical and often incomplete security implementations across device classes (Kouloumpris, 2026). In addition, cost-driven manufacturing favors rapid deployment and mass production over robust security by design. As the IoT develops across consumer, healthcare, industrial and defense ecosystems, attackers increasingly weigh these architectural weaknesses at scale (Mokhonoana, 2026).

However, susceptibility is increasing not only because the volume of devices is increasing, but also because many devices are insecure-by-design or deployed without adequate life cycle security management.

Classification of Vulnerabilities

1. *Device-Level Vulnerabilities:* Device-level deficiencies arise from vulnerable hardware and firmware vulnerabilities. These include weak or missing authentication, weak encryption, insecure boot loadings, and a lack of firmware integrity verification. Many IoT devices remain susceptible due to obsolete or unpatched software components (Mazhar et al., 2023). Resource constraints continue to hinder the implementation of strong security controls (Mazhar et al., 2023).
2. *Network-Level Vulnerabilities:* Network-level vulnerabilities arise from poor segmentation, direct vulnerability of devices to the public Internet, and insecure communication protocols. Fragile network engineering enables adversaries to intercept, manipulate, and disrupt data flows across IoT ecosystems (Vidović, 2025). The interoperability challenges of heterogeneous IoT agreements also create increased attack vectors (Molade, 2025).
3. *Systemic and Supply-Chain Vulnerabilities:* Systemic vulnerabilities emerge when universally deployed IoT devices revolve around shared software components. A prominent example is Ripple 20, a set of 19 zero-day vulnerabilities discovered in the Treck TCP/IP library, disclosed by the JSOF Research Lab in 2020. Ripple 20 affects medical, industrial, consumer, and defense devices embedded with the same vulnerable library. This shows how a single flaw in a shared component can cascade across millions of devices (Harding, 2025).

Several challenges in updating operations worsen systemic vulnerabilities. Many IoT devices lack automated patching mechanisms or require manual intervention, resulting in long

term exposure. The heterogeneity of hardware, firmware, and vendor practices also involves uniform security enforcement (Sharma, 2025).

Attack Surface Abuse: IoT methods frequently develop into various parts of botnets because of evading credentials or weak authentication. The most documented case is the Mirai botnet, which performed large-scale distributed denial-of-service (DDoS) attacks by compromising hundreds of thousands of IoT devices. Mirai demonstrated how vulnerable IoT nodes can be exploited for disruptive cyber operations, including traffic flooding, data exfiltration, and lateral movement inside networks (Swain, 2025).

Consequences of IoT and CPS Vulnerabilities

Vulnerabilities in IoT and CPS environments expose systems to multiple risks, including:

- Compromise of connectivity and man-in-the-middle (MITM) attacks.
- Data breaches, unauthorized access, or manipulation of sensor data.
- Denial-of-service (DoS) or device "bricking" attacks.
- Cascading failures across interdependent smart-city or industrial networks.
- Supply-chain propagation of vulnerabilities embedded in shared components.

Mitigation Strategies and Defensive Recommendations

1. *Identity Management and Cryptographic Controls:* Strong authentication, elimination of default credentials, secure firmware signing, and encrypted communication are essential for reducing common IoT attack vectors (Jimmy, 2025).
2. *Cloud, Fog, and Edge Security Integration:* The combination of cloud fog edge architectures can enable integrated system monitoring, secure update management, and computational offloading for constrained devices. These compositions increase detection and reduce the attack surface (Zhukabayeva, 2025).
3. *Software Diversity and Heterogeneous Architectures:* Avoiding device monocultures and using diverse firmware stacks reduces systemic supply chain risks. Security heterogeneity minimizes the tendency of a single exploit to compromise many devices concurrently (Dev, 2025).
4. *Lightweight Security Techniques:* Weak cryptography, anomaly detection models, and tailored risk assessment protocols facilitate secure operations on resource-limited IoT devices (Pandey, 2025).
5. *Network Segmentation and DDoS Protection:* Segmenting IoT networks, deploying intrusion detection systems (IDS), filtering device onboarding, and applying edge rate limiting help prevent botnet recruitment and large-scale DDoS attacks (Al-Shurbaji, 2025).
6. *Continuous Risk Assessment for IoT Ecosystems:* Predictable risk frameworks that consolidate device dependencies, firmware update cycles, and mission-critical considerations enable holistic security management in IoT environments (Lizut, 2025).

Relevance to Defense and Security Environments

Within unsecure security environments such as smart cities, healthcare IoT, defense platforms, and the Internet of Military Things (IoMT), IoT vulnerability concerns can serve as gateways for intelligence, interruption, and physical danger. However, the protection of IoT deployments requires a security system design, strong identity controls, and secure management protocols.

Table 1. Layered Vulnerability Mapping in IoMT Systems

Layer	Vulnerability	Impact	Example Attack
Device Layer	Weak authentication, unpatched firmware	Device compromise	Botnet infection
Network Layer	Poor segmentation, insecure protocols	Lateral movement	DDoS attack
System Layer	Shared components, software dependencies	Cascading failures	Ripple20
Operational Layer	Lack of monitoring, weak policy enforcement	System wide disruption	Multi vector attacks

Domain Specification

Specifications are domain-specific operational controls that define hard and measurable details, such as configurations or attributes. Specifications are derived from enterprise information security standards, with each domain potentially obtaining unique interpretations of a common standard, depending on each unique environment. This allows for a degree of autonomy in the execution. Care must be taken when deriving specifications to ensure domain-specific interpretations; while meeting the intent of the parent standards, do not cause interdomain incompatibility. To avoid introducing an unidentified risk, the specifications must meet the spirit and intent of the parent standard (Tipton & Krause, 2007).

The CICIoMT2024 dataset was generated using a diverse set of IoMT devices deployed in a controlled laboratory environment. These devices represent typical healthcare connected technologies including wearable sensors monitoring equipment smart cameras and health monitoring platforms. The diversity of hardware devices allows the dataset to reflect realistic operational conditions present in modern IoMT environments.

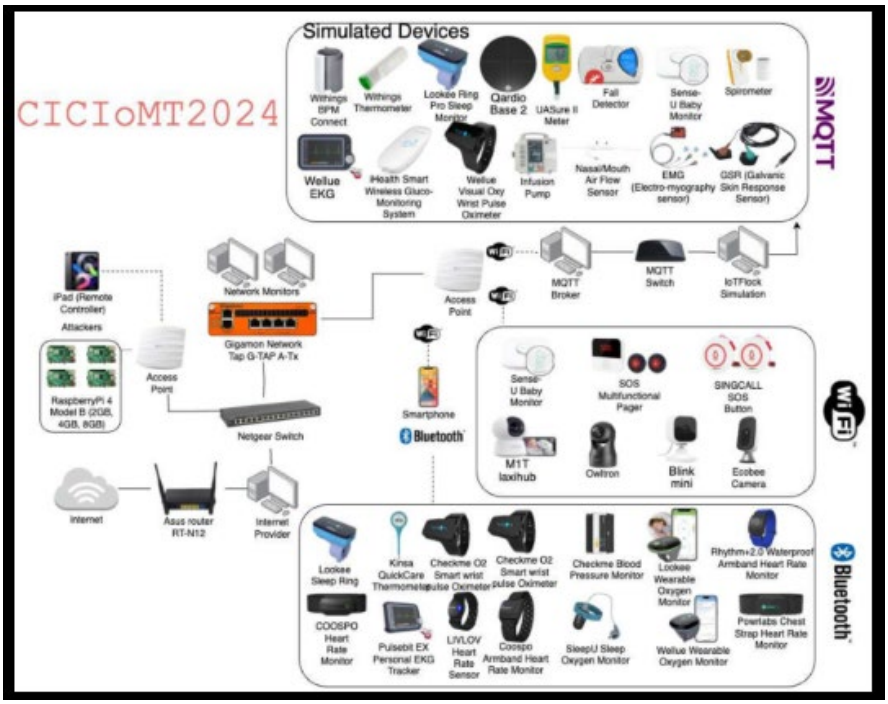


Figure 2. MQTT

Figure 2 shows the IoMT devices used in the CICIoMT2024 dataset including wearable sensors smart monitoring devices cameras and connected healthcare equipment deployed within the experimental testbed. To capture realistic cybersecurity attack traffic an experimental IoMT testbed architecture was developed. The architecture integrates real IoMT devices simulated devices wireless communication protocols and network monitoring infrastructure. A network tap was used to duplicate traffic between the switch and IoMT devices allowing packet capture without interrupting device operations. Attack traffic was generated from controlled attacker nodes connected to the same network environment enabling the dataset to capture a wide range of cybersecurity attack scenarios.

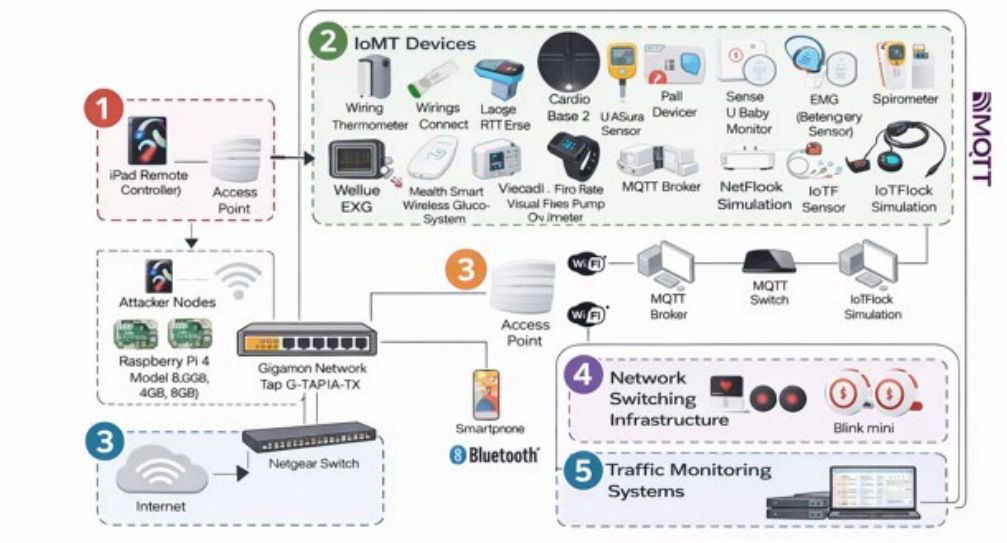


Figure 3. Experimental IoMT Cybersecurity Testbed Architecture

Figure 3 shows the experimental IoMT cybersecurity testbed architecture used for generating the CICIoMT2024 dataset showing IoMT devices, attacker nodes, MQTT communication infrastructure, switching components, and network traffic monitoring systems.

Experimental IoMT Cybersecurity Testbed Architecture

The illustration of experimental architecture used to generate the CICIoMT2024 dataset. The testbed integrates multiple components including attacker nodes, wireless communication channels, IoMT devices, switching infrastructure, and monitoring systems used for capturing network traffic. Architecture allows controlled cybersecurity attacks to be executed against IoMT devices while enabling researchers to capture and analyze the resulting network traffic. The testbed includes a collection of IoMT devices such as wearable sensors, monitoring equipment, and connected healthcare devices.

These devices communicate using wireless technologies including Wi-Fi, MQTT messaging protocols, and Bluetooth connectivity. This heterogeneous communication environment reflects the complexity of real IoMT deployments in healthcare settings. To simulate adversarial activity, attacker nodes are connected to the same network environment as the IoMT devices.

These attacker systems generate malicious traffic including reconnaissance operations, spoofing attacks, denial of service attacks, and MQTT-based flooding attacks. By executing attacks within a controlled environment, the testbed enables the systematic capture of both benign and malicious network traffic.

Network traffic generated by both normal device operation and attack scenarios is transmitted through a network switch and duplicated using a network tap device. The network tap enables packet capture without interrupting the communication between IoMT devices and network infrastructure. Captured traffic is forwarded to a monitoring and data collection system where packet traces are recorded and later processed to construct the CICIoMT2024 dataset. This experimental architecture provides a realistic environment for studying cybersecurity vulnerabilities in Internet of Medical Things ecosystems. By combining real devices, simulated attack traffic, and comprehensive traffic monitoring, the testbed enables the analysis of how cybersecurity threats emerge and propagate across interconnected IoMT systems.

Research Method

This study adopts an experimental cybersecurity analysis approach using the CICIoMT2024 dataset to investigate vulnerabilities in IoMT environments. Rather than relying solely on theoretical modeling, the study examines real network traffic generated within a controlled IoMT test-bed environment that simulates healthcare device communication and cyberattack behavior. The objective is to analyze how vulnerabilities emerge across interconnected system layers including devices, communication protocols, and network infrastructure. This experimental approach enables the identification of attack patterns and system level weaknesses that expand the cybersecurity attack surface in IoMT environments.

Data Collection

This study utilizes the CICIoMT2024 dataset, a benchmark dataset designed for evaluating cybersecurity threats in IoMT environments across multiple communication protocols including Wi-Fi, MQTT, and Bluetooth (Abo-Haat, 2025).

Data Description

Network traffic was captured using a network tap positioned between the network switch and Wi-Fi and MQTT enabled IoMT devices within the experimental environment. The network tap duplicates packet traffic in real time, allowing researchers to capture network communication without interrupting device operations. The following is a quick rundown of documented attacks.

Figure 4. Attack Propagation Flow

The Data Collected

Attacks were conducted on WiFi-enabled IoMT devices and simulated MQTT devices, highlighting the vulnerabilities of both devices. The following is a quick rundown of documented attacks:

- Bluetooth Low Energy devices within the testbed were also subjected to denial-of-service attacks to evaluate vulnerabilities in short range wireless communication used by wearable medical devices.
- Experiments were performed to analyze the behavior of IoMT devices in various scenarios.
- Individual tests and observations were conducted for each device.
- Network traffic was captured from late night to early morning for an empty laboratory.
- All network traffic was captured during the experiment. Researchers can generate lab-network traffic, either actively or passively. The experiment evaluated IoMT functionalities and captured network traffic (Adrović, 2025).

Table 2. The CICIoMT Dataset Defines Attacks As

Category	**Attack Types**
DDoS	SYN Flood, TCP Flood, ICMP Flood, UDP Flood
DoS	SYN Flood, TCP Flood, ICMP Flood, UDP Flood
Recon	Ping Sweep, Vulnerability Scan, OS Scan, Port Scan
Spoofing	ARP Spoofing
MQTT Attacks	Malformed Data, DoS Connect Flood, DDoS Connect Flood, DoS Publish Flood, DDoS Publish Flood

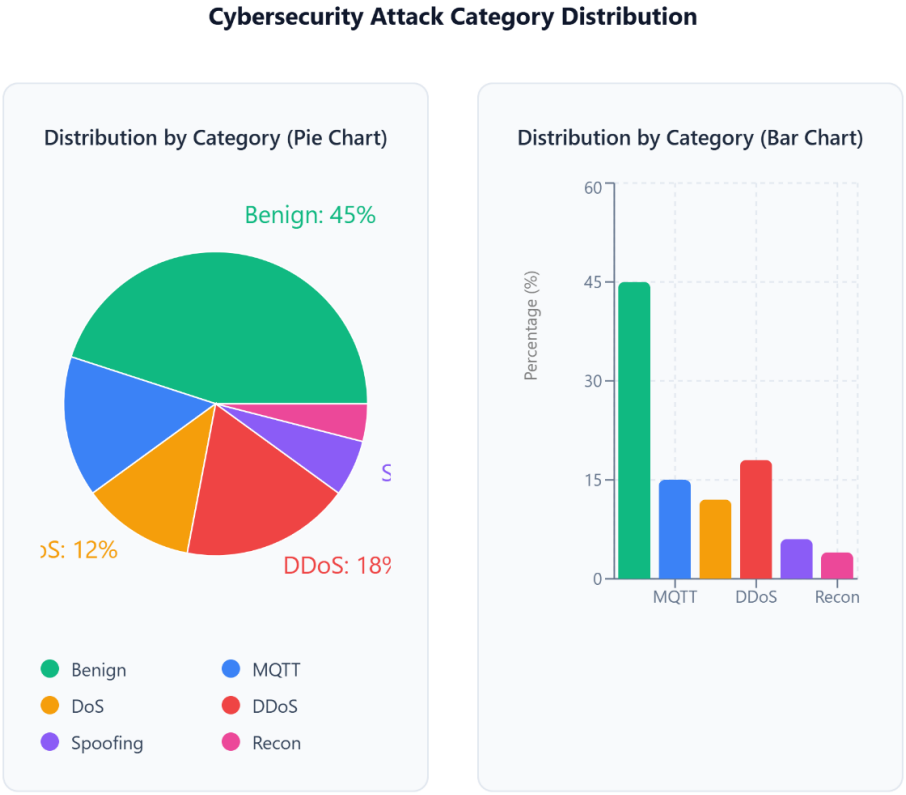
Table 3. Attacks on WIFI MQTT Devices

Category	Types
Malformed Data	TCP flooding
	ICMP flooding
	UDP flooding
DoS Connect Flood	SYN flooding
	TCP flood attack
	ICMP flooding
	UDP flooding
DDoS Connect Flood	Network ping
	Vulnerability check
	OS Scanning
	Scan ports
DoS Publish Flood	ARP spoofing
DDoS Publish Flood	Data error
	Flood DoS Connect
	DDoS attack
	DoS attacks the publishing system
	DDoS flood

Descriptive Statistics

The descriptive statistics of the features extracted from the PCAP files are shown in the table below.

The data distribution for each class is shown in the following charts, and the data comprises MQTT and benign traffic. Nonetheless traffic generated in the multiclass classification can be attributed to benign cases and floods specifically related to MQTT connections. This presentation also highlights the distribution of DoS and DDoS traffic, with UDP and ICMP DDoS floods accounting for the data in a multiclass classification. The data distribution for each class is shown in the following charts.



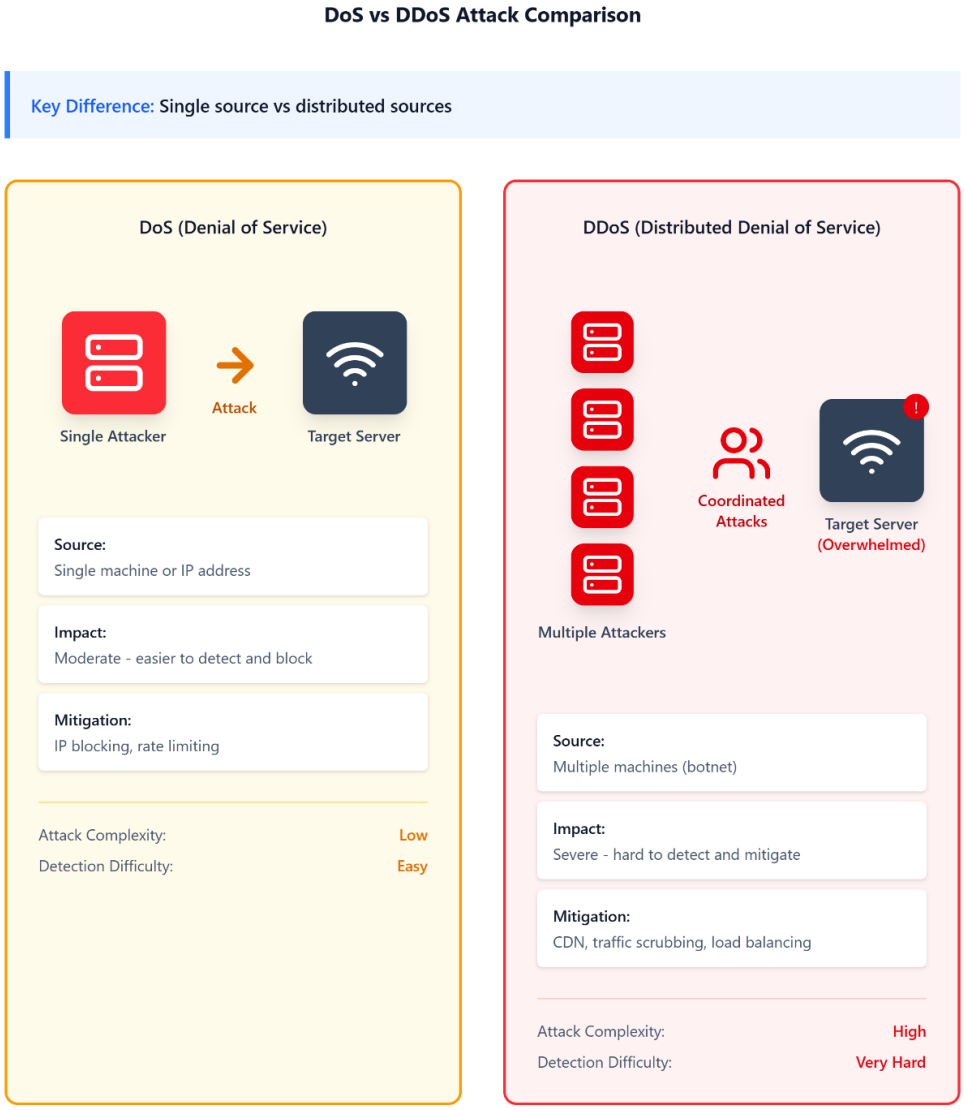
Category	Percentage	Color Code	Description
Benign	45%		Normal network traffic
MQTT	15%		MQTT protocol attacks
DoS	12%		Denial of Service attacks
DDoS	18%		Distributed Denial of Service
Spoofing	6%		Identity spoofing attacks
Recon	4%		Reconnaissance activities

Figure 5. Traffic Distribution

Figure 5 includes the distribution of network traffic classes in the CICIoMT2024 dataset including benign MQTT DoS DDoS spoofing and reconnaissance traffic categories.

Dataset Directory

The CICIoMT2024 dataset contains captured network traffic for Wi-Fi, MQTT, and Bluetooth IoMT devices. The dataset includes benign traffic, attack traffic, and device profiling traffic collected during multiple operational states including power, idle, active, and interaction states. This presentation also highlights the distribution of DoS and DDoS traffic.



Feature	DoS	DDoS
Attack Sources	Single	Multiple (Distributed)
Traffic Volume	Lower	Much Higher
Execution Difficulty	Easy	Requires Botnet
Detection	Simple	Complex
Blocking Method	IP Blacklist	Advanced Filtering

Figure 6. Comparative Analysis

Figure 6 shows the comparative analysis of denial of service and distributed denial of service attack patterns across multiple protocol-based traffic categories.

Figure 7. Mitigation Strategies

In Figure 7, systemic cybersecurity defense architecture for IoMT environments illustrates layered protection across device network edge cloud and governance levels with continuous monitoring and risk management.

Conclusion

Cybersecurity vulnerabilities in modern digital infrastructures increasingly arise from the complexity of interconnected systems rather than isolated technical flaws. This study examined cybersecurity vulnerabilities in IoT and cyber physical environments through experimental analysis of Wi-Fi enabled IoMT devices and MQTT communication networks. The results demonstrate that vulnerabilities at the device level including weak authentication mechanisms unpatched firmware and insecure communication protocols can interact with network level weaknesses such as poor segmentation and exposed services to significantly expand the cyber-attack surface.

The analysis highlights how adversaries exploit these vulnerabilities to conduct DoS and DDoS attacks as well as reconnaissance and spoofing operations. These findings reinforce the need to examine cybersecurity through a systems perspective that accounts for the interactions

between devices networks and operational environments. Effective cybersecurity defenses must therefore extend beyond isolated vulnerability mitigation and incorporate architectural strategies including strong identity management cryptographic controls network segmentation and continuous risk assessment.

Future research should focus on developing adaptive security architectures capable of dynamically identifying and mitigating vulnerabilities across heterogeneous IoT ecosystems. Such approaches will be critical for protecting emerging cyber physical infrastructures including healthcare technologies, smart city systems and critical national infrastructures.

Acknowledgment

The author acknowledges the Canadian Institute for Cybersecurity at the University of New Brunswick for providing the CICIoMT2024 dataset used in this research (Dadkhah et al., 2024).

References

Abo-Haat, M. &. (2025). Advanced multi-protocols framework for cyber attacks detection in IoMT. *International Journal of Intelligent Engineering & Systems, 19*(3).

Adrović, H. (2025). *Enhancing smart home security through IoT device fingerprinting using machine learning: Enhancing smart home security using ML*. Mälardalen University, School of Innovation, Design and Engineering.

Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine learning-based security solutions for IoT networks: A comprehensive survey. *Sensors*, *25*(11), 3341.

Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J. Cyber Secur. Risk Audit*, *2025*(2), 12–26.

Al-Shurbaji, T. A. (2025). Deep learning-based intrusion detection system for detecting IoT botnet attacks: A review. *IEEE Access*, 13, 11792–11822.

Damianou, A. L. (2025). VR-CybSA: Towards virtual reality-enhanced situational awareness in cyber range training. In P*roceedings of the Future Technologies Conference*, 541–557.

Dev, Y. &. (2025). A layered security perspective on the Internet of Things ecosystem: Threat taxonomy, vulnerabilities, and mitigation strategies. *International Journal of Computer Science Engineering Techniques, 9*(6).

Dias, N. I., Vir, D., Kumar, S., Sidhu, K. S., Abdurakhimova, D., & Mannar, B. R. (2026). An In-Depth Analysis of Cybersecurity Risks, Threat Propagation, and Systemic Vulnerabilities in Highly Interconnected Digital Ecosystems. In *Resilient Privacy-Preserving Mechanisms for Digital Identity Management* (pp. 139-170). IGI Global Scientific Publishing.

Edrisi, F. P.-P. (2025). Approaching proactive self-adaptation in nonlinear cyber-physical systems. In *2025 IEEE/ACM 20th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS) IEEE*, 25–31.

Harding, W. H. (2025). *Securing a connected future*. Springer Nature Switzerland. doi: https://doi. org/10.1007/978-3-032-07309-9

Jimmy, M. J. (2025). Identity and access management for IOT devices. *In IoT Security Academic Press*, 137–151.

Kouloumpris, A. G. (2026). Exact, efficient, and reliable multi-objective and multi-constrained IoT workflow scheduling in edge-hub-cloud cyber-physical systems. *IEEE Internet of Things Journal*.

Lizut, R. (2025). Ssecurity challenges of IoT integration in national and state critical infrastructures. *Politics & Security*.

Mallick et al. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News 190*(1), 1–69.

Mokhonoana, K. Z. (2026). Bridging the cybersecurity skills gap for effective cyber audit and governance in the telecommunications sector. *South African Journal of Information Management 28*(1), 2075.

Molade, D. O. (2025). *SoK: A systematic review of malware ontologies and taxonomies and implications for the quantum era*. arXiv preprint arXiv:2509.19650.

Moriano, P. H. (2025). Self-adaptation for cybAdaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature reviewer-physical systems: A systematic literature review. *Artificial Intelligence Review*, *58*(9), 283.

Motlagh, R. R. (2026). Cybersecurity risk management in cooperative intelligent transport systems.

Nithyavani, G. (2025). A comprehensive survey on security and privacy challenges in internet of medical things applications: Deep learning and machine learning solutions, obstacles, and future directions. *IEEE Access*.

Nukpezah, J. A. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In *Smart cities and innovative Urban technologies* (pp. 47–65). Routledge.

Olasehinde, D. O. et al. (2026). Cybersecurity in cyber-physical power systems: Analyzing vulnerabilities, threats, and control structures. *Cluster Computing 29*(3), 133.

Özcan, Ö. (2026). Artificial intelligence in intensive care: Applications, challenges, and future directions—A review. *Northern Journal of Health Sciences 2*(1), 49–59.

Pandey, V. K. (2025). A lightweight framework to secure IoT devices with limited resources in cloud environments. *Scientific Reports*, *15*(1), 26009.

Pundir, A., Singh, S., Kumar, M., Bafila, A., & Saxena, G. J. (2022). Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era. *IEEe Access 10*, 16350–16364.

Raman, R. S. (2025). Cyber attacks through the ages: Impact assessment and defense strategies. In *Cryptography, biometrics, and anonymity in cybersecurity management* (pp.367–394). IGI Global Scientific Publishing.

Sharma, H. K. (2025). Advanced security for IoT and smart devices: Addressing modern threats and solutions. *Emerging threats and countermeasures in cybersecurity*, 191–216.

Sharma, N. & Shambharker, P. G. (2025). Multi-attention DeepCRNN: An efficient and explainable intrusion detection framework for Internet of Medical Things environments. *Knowledge and Information Systems*, *67*(7), 5783–5849.

Swain, P. K. (2025). IoT applications and cyber threats: Mitigation strategies for a secure future. In *Explainable IoT applications: A demystification* (pp. 403–428). Springer Nature Switzerland.

Tipton, H. F., & Krause, M. (2007). *Information security management handbook*. CRC Press.

Verma, N. K. (2025). A systematic review on cybersecurity of robotic systems: Vulnerabilities trends, threats, attacks, challenges, and proposed framework: N. *erma et al. International Journal of Information Security*, *24*(3), 127.

Vidović, N. (2025). Economic aspects of cyber security: Socio-financial consequences of cyber attacks. *International Journal of Contemporary Security Studies*, 105–118.

Vidyalakshmi, G. G. (2025). Digital twins and cyber-physical systems: A new frontier in computer modeling. *Computer Modeling in Engineering & Sciences*, *143*(1), 51.

Zhukabayeva, T. Z. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, 25(1), 213.


Acquisition Research Program
Department of Acquisition, Finance, and Manpower
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net