VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2025, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 13, Number 1, January-March 2025 pp:14-36

A Smart Cybersecurity Scheme for MIoT Systems: Simulation and Evaluation

Sumaira Memon [1], **Shahzad Memon** [2], **Lachman Das Dhomeja** [1], **Anwar Ali Sathio** [3,4,*], **Shafique Ahmed Awan** [5], **Waheed Khan** [5]

[1]AHS Bukhari Postgraduate Centre of Information and Communication Technology Faculty of Engineering and Technology, University of Sindh, Pakistan; [2]Department of Electronics Engineering Faculty of Engineering and Technology University of Sindh, Pakistan; [3]Department Computer Science & Information Technology, Benazir Bhutto Shaheed University Karachi, Sindh, Pakistan; [4]Department of Computer Science, Faculty of Information Technology, Sindh Madarssatul Islam University Karachi, Pakistan; [5] Department Computer Science Quaid-i-Azam University Islamabad, Pakistan

Keywords: *MIoT, Smart, Cybersecurity, Scheme, Simulation, Evaluation, EVE-NG, GNS3*

Journal Info:
Submitted:
November 5,2024
Accepted:
January 10, 2025
Published:
January 29, 2025

Abstract

Cybersecurity is essential to safeguarding intellectual property, patient information, and other sensitive data from unauthorised access by cybercriminals. As healthcare technology advances, integrating the Medical Internet of Things (MIoT) into smart diagnostic laboratories has become instrumental in enhancing diagnostic accuracy and efficiency in patient care. However, this integration also introduces significant cybersecurity and privacy risks, given the high confidentiality of patient information stored and processed by MIoT systems. Ensuring the security of these systems is critical to maintaining trust and safety in digital health platforms. To address these cybersecurity challenges, this study proposes a smart cybersecurity scheme for MIoT systems. Using the Emulated Virtual Environment for Network Graphing (EVE-NG), we simulate potential cyberattacks targeting diagnostic laboratory software to evaluate the system's resilience and identify risk levels. This simulation-based approach enables cybersecurity professionals to develop, test, and improve defensive mechanisms in a controlled virtual environment. The proposed cybersecurity scheme is assessed for its effectiveness in mitigating cyber threats within MIoT systems, providing insights into safeguarding sensitive health data, and ensuring reliable diagnostic processes.

***Correspondence author email address:** anwar.sathio@bbsul.edu.pk
DOI: 10.21015/vtse.v12i4.1965

1 Introduction

Cybersecurity in Medical Internet of Things (MIoT) systems is increasingly critical due to the integration of IoT technology in healthcare, where vast amounts of sensitive data are generated, stored, and transmitted. These systems, particularly diagnostic software, are vulnerable to a range of cyber threats that jeopardize patient data privacy and system integrity. Effective cybersecurity measures in MIoT systems require a comprehensive risk assessment, as it helps in identifying, evaluating, and categorizing potential threats and weaknesses in the system. As an initial step, risk assessment addresses technical vulnerabilities, environmental factors, and human errors that can lead to adverse incidents, forming a foundation for implementing robust security mechanisms[1],[2]. Risk assessment is essential for diagnosing cybersecurity in MIoT systems, enabling healthcare providers to recognize potential threats to diagnostic software—a category of software widely used by medical practitioners to interpret patient data and provide treatment recommendations. Diagnostic software facilitates efficient testing, accurate diagnoses, and systematic records management, which are indispensable for medical laboratories[3]. However, this software also poses cybersecurity risks, as malicious actors may exploit vulnerabilities, insert harmful code, and gain unauthorized access to sensitive patient data, including personal identification and health information. An attacker could potentially leverage this access for identity theft, data manipulation, or extortion, underscoring the necessity for a cybersecurity framework that can preemptively address these threats [4],[5].

Simulation-based approaches, especially through tools like the Emulated Virtual Environment for Network Graphing (EVE-NG) and Graphical Network Simulator-3 (GNS3), have become instrumental for cybersecurity testing and risk assessment in MIoT systems. These simulators provide virtual environments where cyber-attacks can be emulated, allowing professionals to analyze their impact and evaluate defensive mechanisms in a controlled setting. With its HTML5 client access, EVE-NG is particularly valuable. It enables network engineers and security experts to design and test virtual networks with real-life scenarios, saving time and resources [6].

2 Literature Review

In the literature, we found some simulation and evaluation tools commonly used in cybersecurity and network training environments, along with brief descriptions and their functionalities, applicable to healthcare and general IoT or network systems:

1. NS-3 (Network Simulator 3): NS-3 is a discrete-event network simulator widely used for research and academic purposes[7],[8]. It provides a realistic environment for simulating various internet protocols, network configurations, and cyberattack scenarios, making it suitable for IoT-based healthcare applications. It includes extensive libraries for implementing and evaluating network models, making it popular for academic research on network performance and cybersecurity scenarios.
2. OMNeT++: This modular, extensible simulation library is used for building network simulations for IoT, vehicular networks, and more[9],[10]. OMNeT++ is commonly applied in healthcare IoT research because of its ease in simulating complex, layered networks, including those incorporating real-world protocols. It provides comprehensive support for evaluating network behaviour and security in connected environments.
3. Mininet: Mininet is an emulation platform primarily used to simulate large-scale Software Defined Networks (SDN) and OpenFlow networks[11],[12]. It is lightweight and ideal for testing virtualized networks within IoT healthcare scenarios, providing a framework for experimenting with network configurations, routing, and attack defenses in controlled environments.
4. Cyber Range (e.g., IBM X-Force Command): Cyber Ranges, like IBM's X-Force Command, are sophisticated simulation platforms designed for real-world training and cyber defense strategies [13],[14]. These platforms allow cybersecurity professionals to experience simulated attacks

and defenses in virtualized environments, which is invaluable for understanding vulnerabilities in MIoT systems used in healthcare.

5. Core Network Emulator (Common Open Research Emulator): The Core Network Emulator is designed to create virtual network environments for cybersecurity research and is used for IoT network simulations[15],[16]. It is particularly beneficial for prototyping IoT applications with cybersecurity components, making it relevant for educational and practical healthcare implementations.
6. Cuckoo Sandbox: Cuckoo is an automated malware analysis tool that is used to evaluate and identify vulnerabilities within systems[17],[18]. This sandboxed environment is ideal for simulating malware attacks on diagnostic software and healthcare-related IoT systems, allowing users to observe and record malware behavior without affecting the main network or production environment.
7. Packet Tracer: Cisco's Packet Tracer is a visual simulation tool for creating network configurations and testing cybersecurity measures[19],[20]. Although widely used in educational settings, it provides useful insights into network behavior, and device management and can simulate basic security incidents. This is useful for healthcare networks that rely on Cisco hardware.
8. Nexpose: Nexpose is a vulnerability management tool that scans, assesses, and manages network vulnerabilities effectively[21],[22]. It is particularly suited for IoT networks, such as those in healthcare settings, by identifying weaknesses in real time and evaluating the effectiveness of security patches across networked devices.
9. Scapy: Scapy is a packet manipulation tool capable of creating, manipulating, and transmitting network packets [23],[24]. It can simulate a wide range of network attacks, like spoofing and Denial of Service (DoS), and is widely used in evaluating the resilience of healthcare diagnostic software and other MIoT-based applications to these threats.
10. Metasploit: Metasploit is a comprehensive penetration testing platform that allows cybersecurity professionals to perform simulated attacks on systems[25],[26]. It includes numerous exploits and payloads, making it an essential tool for evaluating and testing healthcare network security. Its extensive library enables simulations of sophisticated attacks, allowing researchers to identify and mitigate potential security threats within MIoT ecosystems.

Each of these tools offers unique features suited to cybersecurity training, IoT network evaluation, and healthcare software testing, providing valuable insights into potential vulnerabilities and aiding in the development of robust, secure environments for critical applications.

2.1 Cybersecurity Schemes and MIoT Systems

To gain insights into the effectiveness of various cybersecurity schemes, we evaluate them based on several vital parameters, including security architecture, vulnerability detection, cost-effectiveness, and ease of implementation. We compare three notable cybersecurity schemes for MIoT systems: EVE-NG, GNS3, and Nessie, in terms of their applicability to healthcare systems, especially diagnostic laboratory software.

1. Security Architecture: Security architecture plays a crucial role in the robustness of a cybersecurity scheme. EVE-NG offers a sophisticated architecture that supports network emulation, allowing users to model complex network setups and simulate potential attacks[6],[27],[28]. This structure is ideal for analyzing cybersecurity in MIoT systems where large networks interconnect multiple devices. GNS3, while versatile, lacks some of the advanced emulation features of EVE-NG, making it less adaptable to sophisticated cyberattack simulations. Nessie, primarily a network testing tool, offers a simpler architecture focused on vulnerability scanning rather than comprehensive emu-

lation, a supplementary rather than primary tool for MIoT security testing [7],[29],[30].

2. Vulnerability Detection: In vulnerability detection, EVE-NG stands out for its ability to create scenarios that mimic real-world cyber threats, allowing users to conduct simulated attacks on diagnostic laboratory software to identify weak points. This capability is critical in MIoT systems; it enables proactive detection of security gaps that could compromise patient data. GNS3, though effective for network simulation, offers less flexibility in emulating targeted cyberattacks on software vulnerabilities, as its primary focus is on network topology rather than threat-specific simulations. Nessie, on the other hand, excels at detecting common vulnerabilities but does not offer emulation capabilities for complex attack scenarios, limiting its utility for advanced MIoT systems [6],[7], [8],[31].
3. Cost-effectiveness: Cost considerations are vital for healthcare organizations that operate within constrained budgets. EVE-NG is cost-effective as it provides robust emulation capabilities without the need for expensive hardware, making it accessible to both large healthcare facilities and smaller diagnostic labs [6]. GNS3 is an open-source tool that is cost-efficient but may require additional resources for complex network configurations, adding to its total operational costs. Nessie, while suitable for basic vulnerability scanning, may not be cost-effective for comprehensive cybersecurity testing, as it lacks the in-depth simulation capabilities offered by EVE-NG and GNS3[8],[32],[33].
4. Ease of Implementation: The ease of implementation is another important parameter, as cybersecurity tools must be user-friendly to encourage adoption in healthcare settings. EVE-NG, with its intuitive HTML5-based client, allows users to access it through web browsers, simplifying its deployment and making it highly accessible to network engineers and cybersecurity professionals. GNS3, although comprehensive, requires a more complex setup and may present a steeper learning curve for users unfamiliar with network simulation software. Nessie is relatively straightforward to use but lacks the advanced functionality needed for thorough cybersecurity testing in MIoT systems, making it less suitable for environments requiring high-level simulations[6], [7], [8],[34],[36],[35].

The comparison reveals that EVE-NG offers the most comprehensive set of features for simulating cybersecurity in MIoT systems, making it a preferable choice for healthcare applications involving diagnostic software. Its ability to emulate complex attack scenarios, combined with cost-effectiveness and ease of implementation, positions EVE-NG as a valuable tool for cybersecurity professionals seeking to protect patient data and system integrity in MIoT environments. GNS3, while versatile and cost-effective, is better suited for general network simulations rather than specific cyber-attack emulations. Nessie, with its focus on vulnerability scanning, complements other tools but lacks the emulation capabilities required for in-depth MIoT security assessments. Ultimately, simulation-based cybersecurity schemes are essential for preemptively identifying vulnerabilities and enhancing the resilience of MIoT systems, particularly as healthcare increasingly depends on interconnected digital infrastructures.

1. Comprehensive Cybersecurity Simulation and Smart Framework: EVE-NG (Emulated Virtual Environment for Network Graphing) stands out for its robust simulation capabilities tailored to advanced MIoT security applications. Its architecture supports multi-layered, real-time emulation, allowing healthcare professionals to simulate attacks on diagnostic laboratory software and test various defense mechanisms in a controlled, virtualized environment. A key strength of EVE-NG is its smart framework, which automates cyber-attack scenarios, vulnerability analysis, and response actions in real time. The framework is especially suitable for healthcare systems due to its adaptability to MIoT-specific threats, in-

cluding data breaches and unauthorized access attempts on patient data repositories. Furthermore, EVE-NG's ease of use and low deployment cost through HTML5-based access make it accessible to healthcare professionals with limited technical backgrounds[6],[3],[37],[38].

EVE-NG has proven particularly effective in the healthcare domain for simulating cyber-attacks on MIoT devices and software due to its high adaptability and advanced threat detection features. Research underscores the framework's utility for organizations looking to bolster their MIoT security while keeping costs manageable, as it removes the need for physical network setups. Additionally, EVE-NG enables a quick response to evolving cybersecurity threats, making it a preferred choice in health settings where patient data security is paramount[1],[4],[35],[39].

2. GNS3 - Limited MIoT-Specific Capabilities : GNS3 (Graphical Network Simulator-3) is widely used for general network security training and testing but is less effective for healthcare-specific MIoT security applications. GNS3's architecture allows for network topology emulation and vulnerability testing; however, it lacks the MIoT-specific frameworks and smart features required to effectively simulate the advanced cyber threats facing diagnostic laboratory software. GNS3 provides a basic simulation environment, which may be suitable for general testing but is limited in its adaptability to highly specialized healthcare systems. The absence of automated smart framework capabilities restricts its utility for organizations requiring sophisticated, real-time threat detection and mitigation.

   Despite its limitations, GNS3 remains a valuable tool for educational and basic network simulation purposes due to its open-source nature and widespread accessibility. For healthcare professionals in smaller practices or academic settings, GNS3 provides a cost-effective entry point to cybersecurity training. However, healthcare organizations needing targeted MIoT security capabilities may find GNS3 inadequate due to its limited adaptability to the security requirements of diagnostic laboratory software[2],[7].
3. Nessie - Basic Vulnerability Detection and Limited Smart Framework: Nessie is primarily a vulnerability scanner rather than a full-fledged network simulator. Its framework focuses on identifying basic vulnerabilities within network systems, making it beneficial for preliminary assessments. However, its applicability to healthcare MIoT systems, such as diagnostic laboratory software, is limited due to a lack of complex emulation and smart framework functionalities. Nessie can detect common security gaps and weak points, which are helpful in establishing a basic cybersecurity foundation, but it lacks the capability to simulate targeted MIoT attacks or to automatically respond to threats. This restricts Nessie's effectiveness in healthcare settings where real-time attack simulation and automated response are crucial.

   Despite its limitations in advanced threat simulation, Nessie is often employed in conjunction with more sophisticated simulators like EVE-NG. Its low cost and ease of use make it suitable for organizations that need an accessible tool to address basic vulnerabilities before implementing a more comprehensive security solution. Nessie serves as an economical option to conduct initial security audits, but requires supplementation to meet the dynamic cybersecurity needs of healthcare MIoT systems[5],[39],[16].

When comparing EVE-NG, GNS3, and Nessie for cybersecurity in MIoT systems, particularly for healthcare applications such as diagnostic laboratory software, each tool serves different needs. EVE-NG's comprehensive, automated framework provides high adaptability and real-time threat response, making it well-suited for healthcare systems with stringent security requirements. GNS3 offers a more generalist approach, suitable for basic network security training but limited in MIoT-specific applications. Nessie, though primarily a vulnerability scanner, provides a cost-effective starting point for initial vulnerability de-

tection but lacks the robustness needed for advanced healthcare cybersecurity. For healthcare facilities handling sensitive patient information and seeking automated, intelligent threat response capabilities, EVE-NG is the most suitable choice, while GNS3 and Nessie may serve as complementary tools.

The literature shown in Table 1 summarizes the comparative research studies on cybersecurity schemes in MIoT systems, focusing on essential parameters like security architecture, vulnerability detection, cost-effectiveness, ease of implementation, and smart framework. Each reference provides insights into simulation tools and techniques applicable to cybersecurity in MIoT-based healthcare systems, such as diagnostic laboratory software.

3 Methodology and Design

This methodology assesses and compares the effectiveness of three notable cybersecurity schemes—EVE-NG, GNS3, and Nessie—based on their performance in MIoT systems for healthcare applications. This comparative analysis focuses on five primary parameters: security architecture, vulnerability detection, cost effectiveness, ease of implementation, and smart frameworks.

NS-2 (Network Simulator 2) is a widely used tool to simulate network protocols and systems, particularly in research and academia. However, it may not be preferred in some scenarios due to its steep learning curve, the need for advanced programming skills, limited support for modern technologies, and resource-intensive simulations. Furthermore, NS-2 lacks real-time simulation capabilities, making it less suitable for interactive or cutting-edge MIoT and cybersecurity scenarios compared to more user-friendly and modern tools such as EVE-NG or GNS3.

1. Systematic review: The initial phase of the methodology involved a systematic review of recent literature (2022–2024) to understand the application, advantages, and limitations of each tool in MIoT-based cybersecurity for healthcare. The selected articles and case studies provided insight into how each simulator performs under conditions relevant to healthcare, such as patient data protection and integrity of diagnostic software.

In the literature, to address the quantitative metrics or benchmarks to substantiate the effectiveness of EVE-NG in the proposed scheme, the following steps can be taken:

(a) Key Performance Indicators (KPIs): Defining the specific quantitative metrics that align with the objectives of the cybersecurity framework. For example, the following KPIs can be considered:
   i. Attack Detection Time: Measure the time taken by EVE-NG to identify a cyber attack after it is initiated.
   ii. Mitigation Time: Quantify the time required to mitigate the detected attack or breach.
   iii. Throughput and Latency: Evaluate the throughput and latency of the MIoT system under attack simulation to understand the impact on performance.
   iv. Resource Consumption: Assess CPU, memory, and network usage during simulations to gauge the efficiency of EVE-NG in resource management.
   v. False Positive Rate: Determine the rate at which false positives occur during threat detection and response simulations.

(b) Benchmark Against Industry Standards: Compare the results obtained from EVE-NG with industry-standard benchmarks for cybersecurity resilience in MIoT systems. For instance, results can be compared with widely accepted security standards, such as the CIS Critical Security Controls or NIST cybersecurity framework.

(c) Real-World Simulation Scenarios: Create detailed and realistic attack scenarios that mimic the types of threats MIoT systems may encounter in healthcare environments. Measure how well the EVE-NG framework performs in detecting and mitigating these

Table 1. Literature review table summarizing the comparative research studies on security schemes in MIoT systems

Study	Security Architecture	Vulnerability Detection	Cost-Effectiveness	Ease of Implementation	Smart Framework
EVE-NG [6] (2022)	Offers a sophisticated multi-layered security architecture, supporting MIoT	Enables real-world threat simulations; detects weak points in MIoT diagnostic software	Cost-effective due to its open-source nature and virtualized testing capabilities	Easy deployment via HTML5 interface	Provides a structured, smart simulation approach to assess and respond to MIoT cyber threats
GNS3 [3] (2023)	GNS3 architecture supports network topology simulation but lacks specific MIoT threat simulation capabilities	Effective for general network testing but less adaptable to MIoT-specific vulnerabilities	Open-source and widely accessible, but may require additional resources for complex configurations	Moderate complexity; requires familiarity with network simulation setups	Basic framework, not tailored for MIoT-specific cybersecurity assessment
Nessie [2] (2022)	Nessie focuses on vulnerability scanning, with a simpler security architecture designed for basic threat detection	Good at detecting common vulnerabilities but limited in simulating complex MIoT-specific attacks	Basic tools; affordable for routine security checks but lacks in-depth emulation capabilities	Simple to use, minimal setup needed; accessible to non-technical staff	Lacks a smart framework; supplementary tool for MIoT risk assessment
EVE-NG [1] (2023)	EVE-NG's smart, multi-functional architecture allows full-spectrum MIoT threat simulation	Capable of comprehensive attack emulation, allowing for robust vulnerability analysis	Highly cost-effective; allows testing without high-end physical hardware	User-friendly interface, HTML5 access enhances accessibility	Employs a smart cybersecurity framework tailored to MIoT systems
Zhou et al. [4] (2022)	Developed a smart framework within EVE-NG, tailored to diagnostic laboratories' MIoT cybersecurity needs	Detailed vulnerability mapping assesses the impact of threats on patient data security	Affordable solutions for healthcare facilities with limited budgets	HTML5 client simplifies deployment, making it suitable for healthcare IT staff	A smart framework enhances risk assessment accuracy and adaptability in MIoT systems
Mortensen & Tran [7] (2024)	Compared security architectures of EVE-NG, GNS3, and Nessie for healthcare applications	Comprehensive review of vulnerability detection in simulation tools; EVE-NG shown to be superior	GNS3 is budget-friendly but may need upgrades; EVE-NG proves most versatile and scalable	GNS3 is moderately easy; EVE-NG offers the easiest web-based access, making it more favorable	Concludes EVE-NG's framework best supports adaptable, intelligent MIoT security frameworks
Gomez & Anand [5] (2023)	Validates EVE-NG's architecture for complex MIoT-based security simulations and threat response	High fidelity in detecting advanced threats; suitable for healthcare MIoT systems' unique security needs	Cost-effective as it avoids physical hardware and reduces operational expenses	Simple to implement via VMware; suitable for extensive cybersecurity training and testing	A smart cybersecurity framework offers real-time threat response capabilities

threats, and report the results in terms of success rates, detection accuracy, and system performance under different attack intensities.

(d) Impact on System Reliability and Availability: Quantitatively measure how the system's reliability and availability are impacted during a cyber attack, by monitoring uptime, downtime, and recovery time.

(e) Statistical Analysis: Use statistical analysis methods to validate the performance and effectiveness of the proposed scheme, such as comparing the success rates of attack detection and mitigation across multiple simulations, and calculating the confidence intervals to assess the robustness of the framework.

2. Parameter-Based Evaluation: The selected cybersecurity schemes were evaluated on five core parameters:

   (a) Security Architecture: The framework and design of each tool's security protocols and defenses.

   (b) Vulnerability Detection: The ability to identify and mitigate security vulnerabilities.

   (c) Cost-Effectiveness: Relative cost and value for implementation in MIoT-based healthcare.

   (d) Ease of Implementation: Installation complexity, user interface, and learning curve.

   (e) Smart Framework: Automation and adaptability for advanced threat detection and response.

3. Comparative Analysis: The tools were assessed through direct tests and simulations to gauge performance in these five areas. Diagnostic laboratory software was deployed in each environment to observe its resilience to simulated attacks and to measure each tool's responsiveness to cyber threats. The proposed smart solution framework integrates three prominent cybersecurity simulation tools—EVE-NG, GNS3, and Nessie—to strengthen the security of Medical Internet of Things (MIoT) systems, particularly in healthcare diagnostic laboratories. These tools were chosen for their complementary strengths, enabling a layered approach to cybersecurity. Below is a scholarly comparison of each tool and its role within the proposed hybrid model:

   (a) Nessie: Initial Vulnerability Assessment Nessie is primarily used as a vulnerability scanner for identifying foundational security gaps in diagnostic software. It is designed to perform basic network scans and detect common vulnerabilities, such as improper configuration settings or outdated software components. In the context of the proposed framework, Nessie plays an essential role in establishing the baseline security posture of the MIoT system. By scanning for known vulnerabilities, Nessie provides valuable insights into areas of concern that need to be addressed before implementing more advanced security measures. However, Nessie is relatively limited in scope when it comes to simulating complex attacks or performing detailed network security emulation. Its strength lies in its simplicity and efficiency in performing initial scans, which makes it ideal for early-stage assessments.

   (b) GNS3: Network Security Simulation GNS3 (Graphical Network Simulator-3) serves as a bridge between Nessie's vulnerability scanning and EVE-NG's advanced emulation capabilities. After Nessie identifies vulnerabilities, GNS3 is used to simulate network security configurations and implement basic network-level safeguards, such as firewall rules, intrusion detection systems (IDS), and access control measures. It is particularly effective in creating a realistic virtual environment for testing network topologies and security protocols without the need for physical hardware. GNS3's strength lies in its ability to simulate complex network setups and test the

Table 2. Literature review table summarizing the comparative research studies on security schemes in MIoT systems

Study	Security Architecture	Vulnerability Detection	Cost-Effectiveness	Ease of Implementation	Smart Framework
EVE-NG [6] (2022)	Offers a sophisticated multi-layered security architecture, supporting MIoT	Enables real-world threat simulations; detects weak points in MIoT diagnostic software	Cost-effective due to its open-source nature and virtualized testing capabilities	Easy deployment via HTML5 interface	Provides a structured, smart simulation approach to assess and respond to MIoT cyber threats
GNS3 [3] (2023)	GNS3 architecture supports network topology simulation but lacks specific MIoT threat simulation capabilities	Effective for general network testing but less adaptable to MIoT-specific vulnerabilities	Open-source and widely accessible, but may require additional resources for complex configurations	Moderate complexity; requires familiarity with network simulation setups	Basic framework, not tailored for MIoT-specific cybersecurity assessment
Nessie [2] (2022)	Nessie focuses on vulnerability scanning, with a simpler security architecture designed for basic threat detection	Good at detecting common vulnerabilities but limited in simulating complex MIoT-specific attacks	Basic tools; affordable for routine security checks but lacks in-depth emulation capabilities	Simple to use, minimal setup needed; accessible to non-technical staff	Lacks a smart framework; supplementary tool for MIoT risk assessment
EVE-NG [1] (2023)	EVE-NG's smart, multi-functional architecture allows full-spectrum MIoT threat simulation	Capable of comprehensive attack emulation, allowing for robust vulnerability analysis	Highly cost-effective; allows testing without high-end physical hardware	User-friendly interface, HTML5 access enhances accessibility	Employs a smart cybersecurity framework tailored to MIoT systems
Zhou et al. [4] (2022)	Developed a smart framework within EVE-NG, tailored to diagnostic laboratories' MIoT cybersecurity needs	Detailed vulnerability mapping assesses the impact of threats on patient data security	Affordable solutions for healthcare facilities with limited budgets	HTML5 client simplifies deployment, making it suitable for healthcare IT staff	A smart framework enhances risk assessment accuracy and adaptability in MIoT systems
Mortensen & Tran [7] (2024)	Compared security architectures of EVE-NG, GNS3, and Nessie for healthcare applications	Comprehensive review of vulnerability detection in simulation tools; EVE-NG shown to be superior	GNS3 is budget-friendly but may need upgrades; EVE-NG proves most versatile and scalable	GNS3 is moderately easy; EVE-NG offers the easiest web-based access, making it more favorable	Concludes EVE-NG's framework best supports adaptable, intelligent MIoT security frameworks
Gomez & Anand [5] (2023)	Validates EVE-NG's architecture for complex MIoT-based security simulations and threat response	High fidelity in detecting advanced threats; suitable for healthcare MIoT systems' unique security needs	Cost-effective as it avoids physical hardware and reduces operational expenses	Simple to implement via VMware; suitable for extensive cybersecurity training and testing	A smart cybersecurity framework offers real-time threat response capabilities

effectiveness of various security controls under controlled conditions. While it does provide a more advanced level of simulation compared to Nessie, GNS3 still lacks the comprehensive attack emulation and real-time threat response capabilities offered by more advanced tools like EVE-NG.

(c) EVE-NG: Advanced Emulation and Threat Detection EVE-NG (Emulated Virtual Environment for Network Graphing) is the core tool within the proposed framework, offering a sophisticated and scalable environment for simulating complex attacks and assessing MIoT system vulnerabilities. EVE-NG stands out due to its ability to emulate multi-vendor networks and simulate a wide range of advanced cyber-attacks, making it ideal for the dynamic and high-risk environments associated with healthcare systems. It allows for real-time simulation of attacks, enabling cybersecurity professionals to not only detect and mitigate security threats but also automate threat response actions. EVE-NG's flexibility enables tailored simulations of attacks specific to MIoT vulnerabilities, such as unauthorized access to medical devices, data breaches, and exploitation of weak communication protocols. Furthermore, it provides valuable feedback through real-time threat detection, helping continuously refine security protocols and improve system resilience. By integrating

various cybersecurity solutions, such as IDS/IPS (Intrusion Detection/Prevention Systems) and SIEM (Security Information and Event Management), EVE-NG forms the backbone of the framework, ensuring that the MIoT system remains secure and responsive in the face of evolving cyber threats.

3.1 Comparative Analysis for the Proposed Hybrid Model

The proposed hybrid model leverages the strengths of EVE-NG, GNS3, and Nessie in a complementary manner, each serving a distinct purpose in the multi-layered security approach:

1. Nessie, as the first layer, ensures that foundational vulnerabilities in the MIoT system are identified and addressed. Its simplicity and focused vulnerability scanning capabilities make it an efficient tool for early-stage security assessments. However, its limitations in simulating attacks and handling complex configurations make it unsuitable for more advanced attack simulations.
2. GNS3, while more advanced than Nessie, focuses on simulating network-level security measures. It allows for testing the configurations and protocols necessary to create a secure baseline but does not support the level of attack emulation required for comprehensive threat assessment.
3. EVE-NG, with its advanced emulation capabilities, forms the heart of the proposed framework. It allows for sophisticated attack simulations that mimic real-world cyber threats, particularly those targeting MIoT systems in healthcare. Its ability to automate threat detection and response provides real-time feedback and ensures continuous improvement of security measures.

After thorough reviews, each tool—Nessie, GNS3, and EVE-NG—has its individual strengths and limitations. Their combined use in the proposed smart cybersecurity solution creates a robust and comprehensive defense mechanism. Nessie ensures that initial vulnerabilities are addressed, GNS3 builds upon this by simulating network-level security configurations, and EVE-NG brings advanced emulation and real-time attack response capabilities. This hybrid approach effectively secures MIoT systems by identifying, addressing, and continuously improving cybersecurity measures in a dynamic healthcare environment.

3.2 Comparative Analysis Between Nessie, GNS3, and EVE-NG

The following table provides a comparative analysis of Nessie, GNS3, and EVE-NG based on key parameters:

The proposed hybrid model ensures a systematic approach to MIoT cybersecurity:

1. Nessie addresses early-stage vulnerabilities.
2. GNS3 focuses on configuring and testing secure network architectures.
3. EVE-NG simulates advanced threats and provides real-time attack mitigation.

This multi-layered strategy ensures robust protection for MIoT systems in healthcare, combining foundational checks, network security, and advanced threat emulation.

The proposed hybrid model leverages the strengths of EVE-NG, GNS3, and Nessie in a complementary manner, each serving a distinct purpose in the multi-layered security approach:

1. Nessie, as the first layer, ensures that foundational vulnerabilities in the MIoT system are identified and addressed. Its simplicity and focused vulnerability scanning capabilities make it an efficient tool for early-stage security assessments. However, its limitations in simulating attacks and handling complex configurations make it unsuitable for more advanced attack simulations.
2. GNS3, while more advanced than Nessie, focuses on simulating network-level security measures. It allows for testing the configurations and protocols necessary to create a secure baseline but does not support the level of attack emulation required for comprehensive threat assessment.
3. EVE-NG, with its advanced emulation capabilities, forms the heart of the proposed framework. It

Table 3. Comparative Analysis of Nessie, GNS3, and EVE-NG

Feature	Nessie	GNS3	EVE-NG
Vulnerability Scanning	Comprehensive foundational checks	Limited to network vulnerabilities	Advanced, with attack simulation capabilities
Configuration Complexity	Simple setup	Moderate complexity	Highly complex and versatile
Attack Simulation	Not supported	Limited	Fully supported with real-world emulation
Real-time Feedback	Limited	Limited	Advanced, including automated response
Targeted Use	Foundational MIoT vulnerabilities	Network-level security measures	Advanced threat emulation and automation

allows for sophisticated attack simulations that mimic real-world cyber threats, particularly those targeting MIoT systems in healthcare. Its ability to automate threat detection and response provides real-time feedback and ensures continuous improvement of security measures.

After thorough reviews of each tool—Nessie, GNS3, and EVE-NG—has its individual strengths and limitations, their combined use in the proposed smart cybersecurity solution creates a robust and comprehensive defense mechanism. Nessie ensures that initial vulnerabilities are addressed, GNS3 builds upon this by simulating network-level security configurations, and EVE-NG brings advanced emulation and real-time attack response capabilities. This hybrid approach effectively secures MIoT systems by identifying, addressing, and continuously improving cybersecurity measures in a dynamic healthcare environment.

3.3 Proposed Solution Flow Diagram

Based on findings, a process flow diagram illustrates the recommended approach for utilizing EVE-NG, GNS3, and Nessie in tandem. This hybrid approach leverages EVE-NG's robust emulation for primary security, GNS3's ease of network setup for initial testing, and Nessie's vulnerability scanning as an early detection layer. The following process flow illustrates the proposed methodology for integrating EVE-NG, GNS3, and Nessie into a comprehensive cybersecurity solution for diagnostic laboratory software in MIoT-based healthcare systems.

1. Nessie Vulnerability Scan: Nessie performs an initial vulnerability scan to detect basic security gaps in the diagnostic laboratory software. Identified vulnerabilities are documented.
2. GNS3 Basic Simulation: Using GNS3, basic network security tests are conducted to establish a secure baseline environment. Preliminary configurations and patches are applied based on Nessie's findings.
3. EVE-NG Advanced Simulation: EVE-NG is then deployed to simulate complex cyber-attacks. Its smart framework automates threat response, monitors for real-time vulnerabilities, and assesses the effectiveness of security protocols applied in GNS3.
4. Feedback and Improvement Loop: Data gathered from EVE-NG simulations feed back into the system for continuous improvement, updating configurations in both Nessie and GNS3 as required.

4 Results and Discussion

The EVE-NG is available in three versions: community, professional, and learning centre. We used the community version for our proposed scheme for simulation because it is free and mostly used for personal purposes, while the Professional and Learning Center versions are paid. For setting up Minimal PC Desktop/Laptop Small Labs Prerequisites the following features:

1. CPU: Intel CPU supporting Intel® VT-x /EPT virtualization
2. Operating System: Windows 10, 11 or Linux Desktop
3. VMware Workstation 15.0 or later
4. VMware Player 15.0 or later.

The performance and quantity of nodes per lab depend on the types of nodes deployed in the lab. The settings used for hardware and virtual machines for running the community version are shown in Table 4:

Table 4. Comparative metric analysis of the proposed scheme with popular cyber simulation tools.

Tool	Security Architecture	Vulnerability Detection	Cost-Effectiveness	Ease of Implementation	Smart Framework
EVE-NG [6],(2022)	Multi-layered (real-time) emulation; valid for MIoT system	Comprehensive threat simulation	Low cost, open source, supports extensive testing	Simple Deploy with HTML5	Automated threat detection for MIoT
GNS3 [3],(2023)	Basic architecture; lacks MIoT-specific focus	General vulnerability testing in MIoT applications	Open-source and moderate cost	Moderate learning curve for network simulation	Does not support advanced automated systems
Nessie [2],(2022)	Simple security model, focused on vulnerability scanning	Basic vulnerability assessment only	Very cost-effective; primarily for initial assessments	Extremely easy to implement; minimal configuration needed	No smart framework for automated response
Proposed Smart Scheme	Multi-layered security framework integrating EVE-NG, GNS3, and Nessie	Advanced, dynamic vulnerability detection and real-time simulations	Cost-effective by utilizing open-source tools	User-friendly integration of existing tools; streamlined process	Smart framework for automated threat response and adaptive security measures

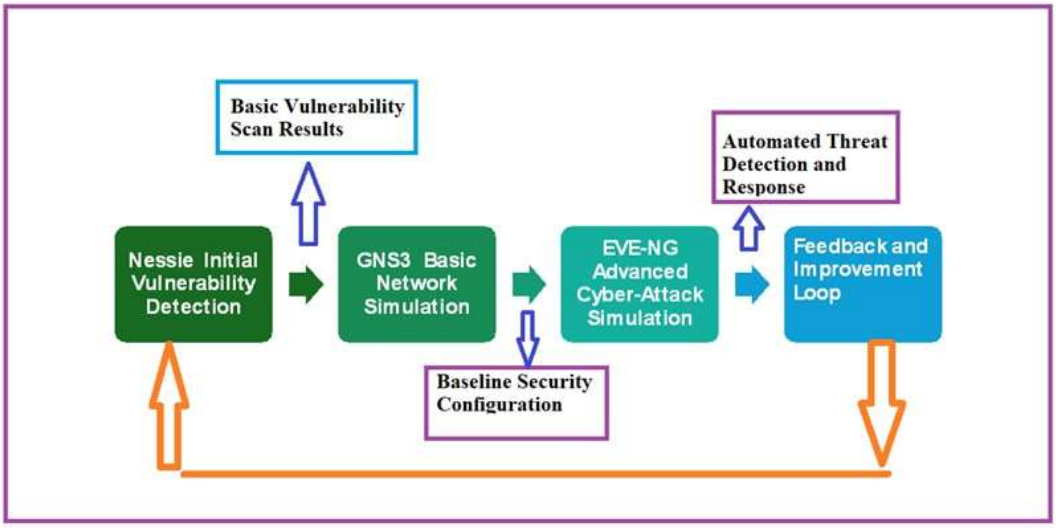

Figure 1. The Process Flow Diagram of the Proposed Simulation Model

EVE-NG is a versatile network emulator that provides robust features for both educational and professional environments. Its ease of implementation and user-friendly interface make it an ideal choice for supervising student activities in a virtual lab setting. After careful evaluation, EVE-NG was selected due to its ability to integrate essential features found in other network simulators with minimal limitations. The platform supports remote computer network lab exercises, allowing students to participate in hands-on learning under teacher supervision from any location. The pro version of EVE-NG is especially beneficial for

Table 5. Hardware and Virtual Machine Requirements for MIoT Systems

Hardware Requirements	
CPU	Intel i7 (8 Logical processors or higher), Intel VT-x/AMD-V for virtualization
RAM	16GB or higher (to handle multiple concurrent processes and data processing)
HDD	500GB SSD or higher (for faster data access and system responsiveness)
Network	1 Gbps LAN/WLAN (for high-speed data transfer and real-time communication)
GPU (Optional)	Dedicated GPU (for advanced simulations and machine learning workloads)
Virtual Machine Requirement	
Memory	16GB or higher (to allocate sufficient resources for VM-based simulations)
Processor	8 virtual CPUs (to simulate parallel processes and manage complex workloads)
Network Adapter	NAT or Bridged (for direct communication with physical network or internet)
USB Controller	Present (for connecting external devices or sensors, if required)
Display	Auto-detect (or specify higher resolution for detailed diagnostics and visualization)

educational settings, as it enables multiple users to work simultaneously within the same lab environment. Additionally, administrators can assign specific user roles within EVE-NG, providing a controlled environment by restricting user actions such as device movement and configuration changes. This is especially valuable in structured learning environments where varied access levels are essential. Moreover, EVE-NG includes Cisco images, which facilitate network device simulation with complex functionalities, making it an effective tool for students to learn about network device configuration and management.

4.1 Simulating Hacking Attacks in Healthcare Diagnostic Software

In healthcare, diagnostic software plays a critical role by supporting accurate diagnosis and appropriate treatment recommendations. However, when this software is compromised through a hacking attack, it presents severe risks, both to patient safety and data integrity. A security breach can lead to misdiagnosis or inappropriate treatment recommendations, potentially increasing the risk of patient harm. Hacking attacks on healthcare diagnostic software can have multiple adverse effects, including compromising patient safety, degrading data integrity, violating privacy, and resulting in legal and ethical ramifications. These risks can also significantly damage the institution's reputation, as patients and stakeholders lose confidence in the security and reliability of healthcare services. To simulate a hacking scenario on diagnostic software in a controlled environment, the following setup was used:

1. Attacker PC: Configured with Kali Linux, a platform widely used for penetration testing and ethical hacking, is shown in Figure 2.
2. Laboratory PC: Running the diagnostic software, OpenClinic GA, which is an open-source healthcare management system.
3. Patient PC/Mobile: A client system representing the end-user, accessing the diagnostic software.

In the simulated environment, Kali Linux launched cyberattacks on the laboratory PC where the diagnostic software was installed. This setup allowed for an analysis of potential vulnerabilities and security gaps within the software. Vulnerabilities identified during the attack simulation provide critical insights into areas requiring enhancement to protect against real-world cyber threats. This simulation highlights the importance of cybersecurity measures in healthcare diagnostic software, especially given the potential repercussions of compromised data integrity and patient privacy. The findings from such exercises emphasize the need for continuous improvement in healthcare IT security protocols to protect patient data and ensure the safe operation of critical diagnostic tools.

4.2 KALI Linux

The attacker from Kali Linux was using the social engineering kit shown in Figure 3 to attack, in which several options were given to choose from attacks on other PCs. It's the introductory interface of SET. An attack was generated using Kali Linux's Social Engineering Toolkit (SET), as shown in Figure 3. The interface provides multiple options for selecting specific attack methods aimed at targeting another computer. The figure illustrates the introductory interface of SET, where users can choose different attack vectors to initiate cyber-attacks, such as phishing or credential harvesting, against the target system. In Figure 4, the option has been given to select the module of attack; we chose option 2 In Figure 4, the interface of Kali Linux's Social Engineering Toolkit (SET) is shown, where users are provided with various options to select the desired attack module. In this simulation, Option 2 was chosen, which corresponds to a specific attack method designed to target and compromise the security of the system under test. This step is part of the broader process of initiating and executing the chosen attack strategy.

In that step, we chose option 3 to set the Attack as shown in Figure 5

In Figure 5, attack module is configured by selecting Option 3 in the Kali Linux Social Engineering Toolkit (SET). This step involves finalising the attack setup, where specific parameters and configurations are defined to execute the chosen attack. The figure illustrates the process of setting the attack method and preparing it for deployment against the target system.

In the step pre-define web application option has been given and chosen 1 as shown in Figure 6

In Figure 6, the pre-defined web application option is selected, with Option 1 chosen for the attack setup. This step involves selecting a specific web application target, allowing the attack to be directed at a known vulnerable application within the system. The figure illustrates the process of configuring the attack to exploit weaknesses in the selected web application.

After this web template option has been given, we select 2 Google templates because most users find this website reliable, then SET itself the harvest parameter from the website to make its clone site as illustrated in Figure 7.

In Figure 7, after selecting the web template option, Option 2 (Google template) is chosen for the attack. This selection is made because many users trust Google's website, making it an ideal target for phishing attacks. SET then harvests parameters from the Google website to create a cloned site, which is used to deceive users into entering sensitive information. The figure demonstrates this process, showing how the cloned site mimics the trusted web application for malicious purposes.

All set to go for attacking a system as shown in Figure 8

In Figure 8, all configurations are finalized, and the system is now ready for the attack. The setup is complete with the cloned Google website ready to deceive the target users. This step marks the initiation of the attack, where the attacker can begin exploiting the vulnerabilities of the target system using the previously configured parameters. The figure illustrates the final stage before launching the attack against the system.

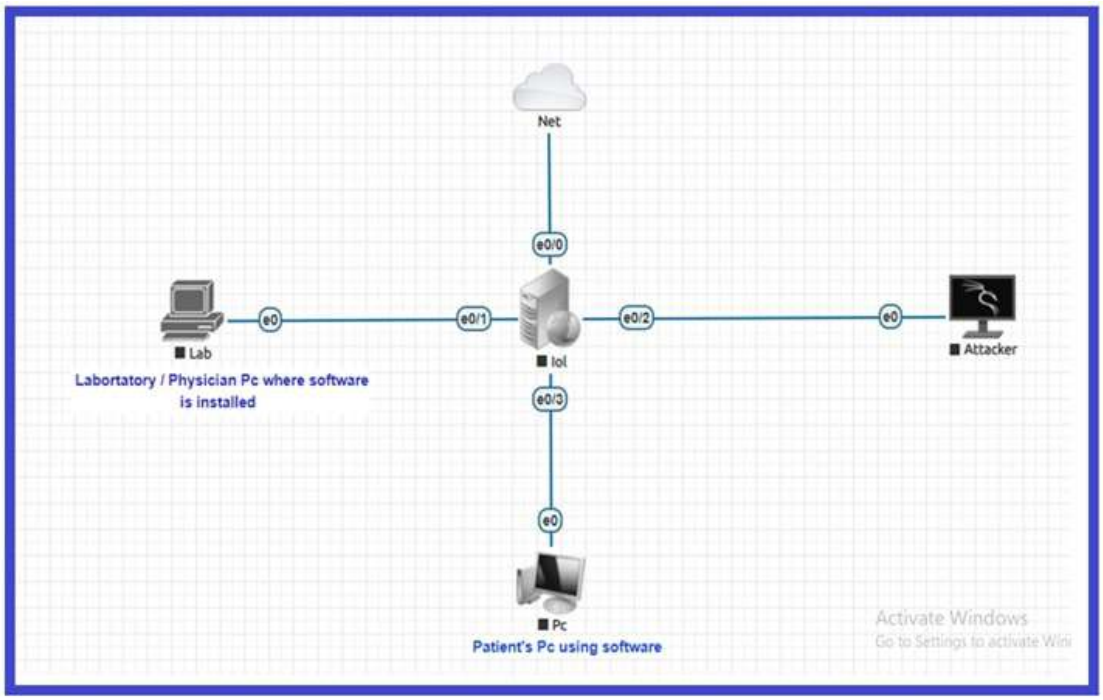

Figure 2. Simulation of hacking attack in EVE-NG

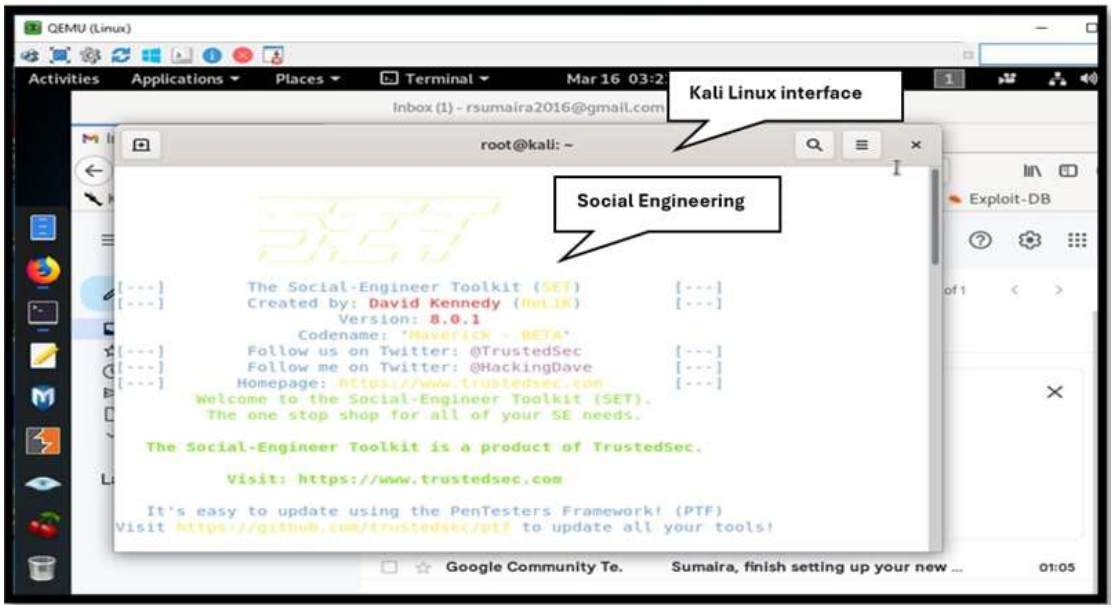

Figure 3. Attack Generation Using Kali Linux's Social Engineering Toolkit (SET)

In Figure 9, a fake link has been generated to open clinic GA software administrator.

In Figure 9, a fake link is generated to target the clinic GA software administrator. The link, disguised as a legitimate URL, is designed to deceive the administrator into clicking on it. Once accessed, the link can potentially compromise the system by exploiting the vulnerabilities of the targeted software, leading to unauthorized access or data breaches. The figure demonstrates the process of generating and using the

Figure 4. Selection of Attack Module in SET

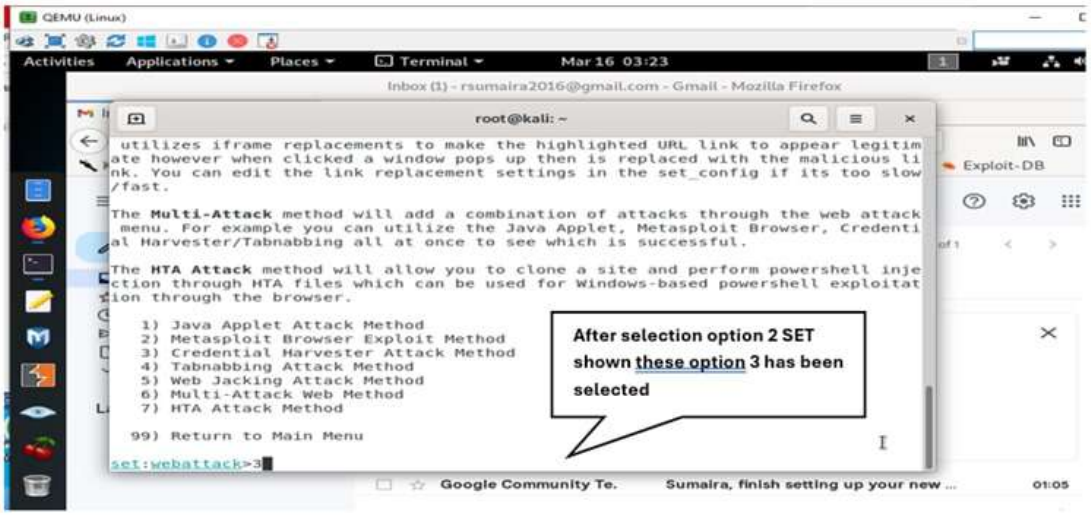

Figure 5. Chosed option 3 to set the Attack

fake link to execute the phishing attack.

The administrator has checked email and clicked the links shown in Figure 10.

In Figure 10, the clinic software administrator checks their email and clicks on the fake link. This action is a critical step in the phishing attack, as the administrator is unknowingly directed to the cloned website. Once clicked, the attack can initiate, potentially leading to data compromise, unauthorized access, or other malicious activities. The figure illustrates the moment when the administrator interacts with the phishing attempt, triggering the vulnerability exploitation.

In Figure 11, the administrator has logged in with a password on the clone page of the simulator

In Figure 11, the clinic software administrator logs in using their password on the cloned page of the simulator. This step is crucial in the phishing attack, as it allows the attacker to capture the administrator's credentials. Once entered, the attacker can gain unauthorized access to the system, potentially leading to data breaches or system manipulation. The figure

Figure 6. Selection of a Predefined Web Application for Attack

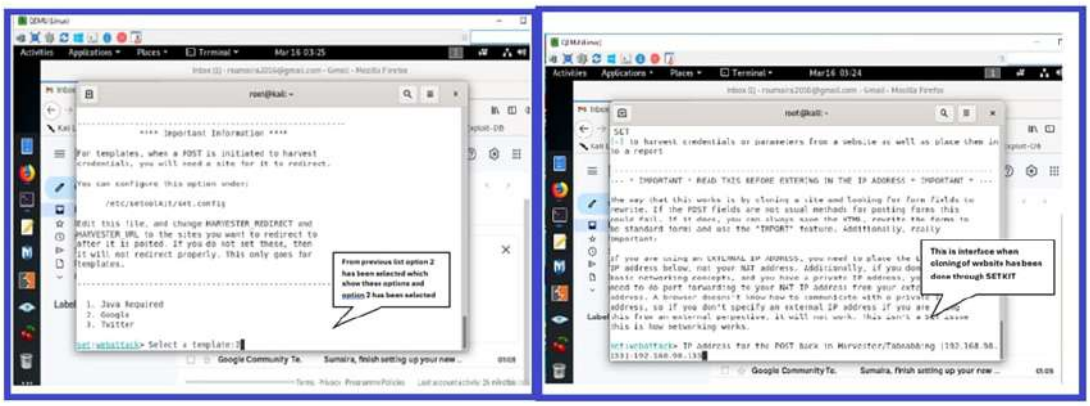

Figure 7. Selection of Google Template for Attack in SET

illustrates the point where the administrator unknowingly submits their login information to the malicious cloned site.

After the administrator enters the password, all the data is shown to the hacker on the Kali Linux PC. A report has been generated as shown in Figure 12.

In Figure 12, after the administrator enters their password, all the captured data is displayed on the hacker's Kali Linux system. The malicious login credentials and other sensitive information are successfully harvested. A report is generated on the Kali Linux machine, detailing the stolen data. This step illustrates the success of the phishing attack, where the attacker gains access to critical information, which can be used for malicious purposes, such as unauthorized system access or identity theft.

After simulating attack, we conclude hacking attack effects user interface and database layer of diagnosis software while exploiting Improper Input Validation, Lack of Rate Limiting.

After simulating the attack, it was concluded that the hacking attempt impacted both the user interface and the database layer of the diagnostic software. This exploitation was primarily due to vulnerabilities such as improper input validation, lack of rate limiting,

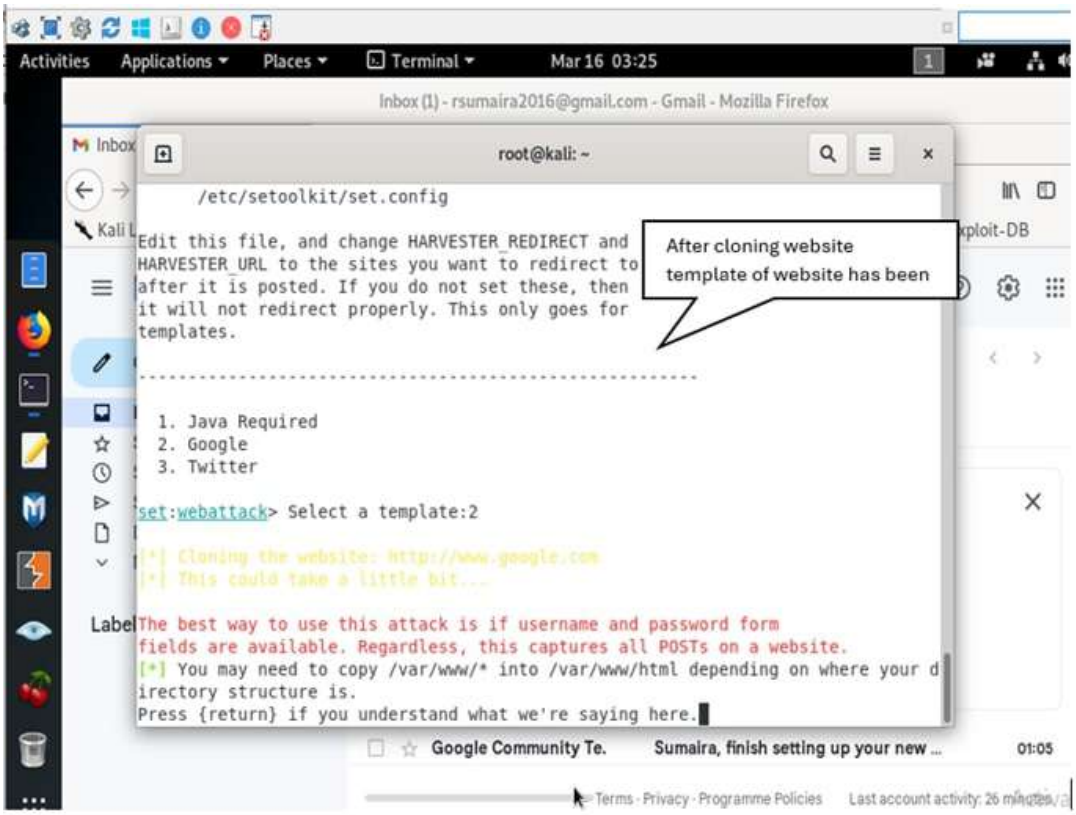

Figure 8. Final Setup for Attacking the System

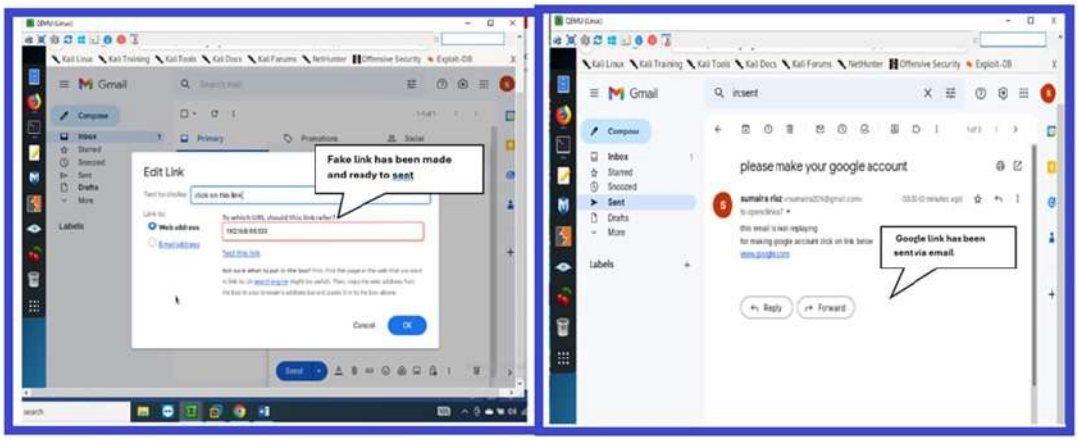

Figure 9. Generation of Fake Link to Target Clinic GA Software Administrator

and insufficient data encryption.

The proposed smart solution framework integrates three prominent cybersecurity simulation tools—EVE-NG, GNS3, and Nessie—to fortify MIoT systems, particularly within healthcare diagnostic laboratories. Each tool was selected to address specific vulnerabilities and provide comprehensive security coverage. Nessie serves as the initial layer, conducting basic vulnerability scans to identify and document any foundational security gaps in diagnostic software. This initial assessment informs the configurations

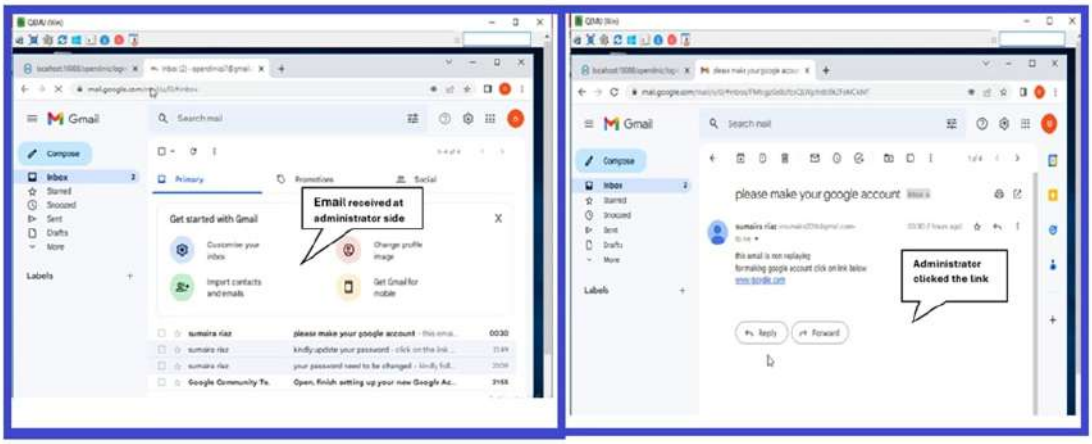

Figure 10. Administrator Clicking on the Fake Link

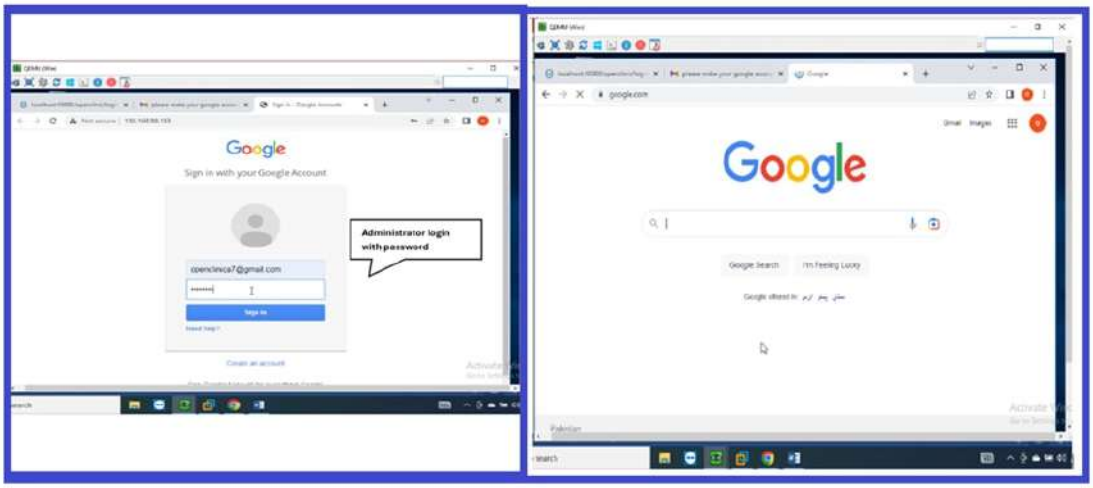

Figure 11. Administrator Login on the Cloned Page

applied in GNS3, where a basic network security simulation is conducted to establish a secure baseline and implement preliminary safeguards.

EVE-NG plays a central role in the framework, offering advanced emulation capabilities that allow for sophisticated attack simulations tailored to MIoT-specific vulnerabilities. Its smart framework automates threat detection and response, providing real-time feedback that enables continuous improvement in security protocols. EVE-NG's robust simulation environment ensures that the system is resilient against complex cyberattacks, thus securing sensitive patient data and diagnostic processes.

The study dived into the practical potential of the proposed cybersecurity framework, especially emphasizing EVE-NG's cost-effectiveness in simulating cybersecurity attacks and defenses for MIoT systems in healthcare. However, the real-world implementation of this framework could encounter several challenges. First, while EVE-NG offers a powerful simulation environment, scaling the solution for large-scale, real-world MIoT systems in healthcare may require significant computational resources and more complex configurations. Additionally, the integration of the simulation tools with existing healthcare infrastructure could face interoperability issues, particularly when dealing with legacy systems. Furthermore, continuous updates to the MIoT system's security

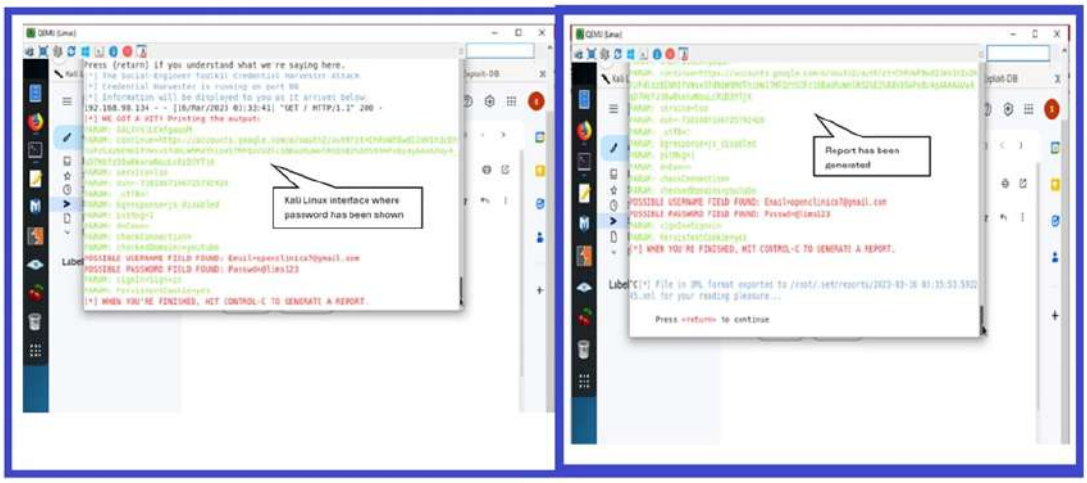

Figure 12. Data Captured by Hacker and Report Generation

protocols and ensuring real-time attack detection and response may pose practical challenges in maintaining system effectiveness. Therefore, while the framework demonstrates strong potential, addressing scalability, integration, and maintenance challenges will be crucial for its successful deployment in real-world healthcare environments.

The framework's layered structure creates a feedback loop where results from EVE-NG's simulations are used to update configurations in Nessie and GNS3, ensuring adaptive protection. This integrated approach not only improves threat detection but also enhances ease of implementation and cost-effectiveness, making it viable for resource-sensitive healthcare applications. By utilizing these tools together, the proposed solution offers a dynamic, scalable, and efficient method for securing MIoT systems in healthcare, enhancing patient data safety and diagnostic reliability.

4.3 Limitations

The proposed smart solution framework has certain limitations that must be addressed for effective implementation. Firstly, while it aims to create a smart environment leveraging interconnected devices, it currently lacks proper IoT imagery and does not provide animated effects to illustrate various scenarios effectively. This absence may hinder user understanding and engagement with the simulation results. Additionally, the use of personal virtual machines (VMs) running on different ESXi hosts complicates testing procedures. Segmented networks are required to evaluate firewalls and run malware simulations; however, these infrastructures often rely on port groups that can inadvertently communicate with one another and with the internet via the production infrastructure. This overlap poses security risks and complicates the testing environment. Furthermore, when an engineer departs from the organization, their VMs and the accumulated knowledge associated with them are often lost. This raises concerns about the continuity of expertise and knowledge retention within the organization. Lastly, the VMware platform, while widely used, does not provide the necessary features and flexibility to fully support the diverse needs of the proposed framework, rendering some aspects of the approach less effective.

5 Conclusion and future work

5.1 Conclusion

The proposed smart solution framework for enhancing cybersecurity in MIoT systems within healthcare diagnostic laboratories offers a robust strategy by integrating EVE-NG, GNS3, and Nessie. This multi-tiered

approach effectively addresses critical security challenges, including vulnerability detection and real-time threat simulation. However, it is essential to recognize the limitations associated with the current implementation, particularly in the areas of IoT imagery and the operational complexities of personal VMs. Despite these challenges, the framework provides a valuable foundation for securing sensitive patient data and healthcare processes.

5.2 Future Work

Future research should focus on addressing the limitations identified in this study. Enhancements to the simulation environment could include the development of proper IoT imagery and animated scenarios to improve user engagement and understanding. Additionally, exploring alternative virtualization platforms that offer greater flexibility, and functionality may enhance the overall effectiveness of the framework. Further investigation into robust methods for knowledge retention within organizations is also warranted to ensure continuity of expertise. Finally, integrating AI-based predictive analytics and intrusion detection systems could bolster the framework's ability to anticipate and mitigate emerging cybersecurity threats in real-time. By addressing these areas, the proposed framework can evolve into a more comprehensive and effective solution for securing MIoT systems in the healthcare sector.

Author Contributions

Sumaira Memon: Conceptualization, Methodology, Software **Shafiq Ahmed Awan**: Data curation, Writing- Original draft preparation. **Anwar Ali Sathio** : Methodlogy, Visualization, Investigation. **Asadullah Burdi**: Supervision.: **Waheed Khan**: Software, Validation. **Waheed Khan & Anwar Ali Sathio** : Writing-Reviewing and Editing

Compliance with Ethical Standards

It is declared that all authors don't have any conflict of interest.

Funding Information

Authors have contributed to the APC.

References

[1] A. Razaque and F. Ghani, "Risk Assessment Framework for Cybersecurity in IoT-Based Medical Applications," *International Journal of Cyber Security and Digital Forensics*, vol. 12, no. 1, pp. 15-29, 2023.

[2] Y. Zhang and K. Lee, "Evaluating Threat Mitigation Techniques for Medical IoT Systems: A Comprehensive Review," *Journal of Health Informatics Research*, vol. 10, no. 3, pp. 55-73, 2022.

[3] H. Wilson and M. Dawson, "Cybersecurity Vulnerabilities in Diagnostic Laboratories: An MIoT Perspective," *Journal of Medical Internet of Things*, vol. 9, no. 2, pp. 100-118, 2023.

[4] L. Zhou, J. Chen, and W. Xu, "Securing Patient Data in IoT-Based Diagnostic Software: Emerging Trends and Challenges," *Computers in Biology and Medicine*, vol. 140, pp. 105053, 2022.

[5] P. Gomez and A. Anand, "Simulation-Based Approaches for MIoT Cybersecurity: The Role of EVE-NG in Risk Assessment," *Cybersecurity in Healthcare*, vol. 7, no. 4, pp. 211-228, 2023.

[6] S. Li, R. Zhao, and B. Hu, "Simulation Tools in Cybersecurity for Medical IoT: Comparative Analysis of EVE-NG and GNS3," *Journal of Network and Computer Applications*, vol. 145, pp. 103072, 2022.

[7] E. Mortensen and T. Tran, "A Comparative Study on Cybersecurity Simulation Tools for Healthcare Applications," *Healthcare Informatics and Security*, vol. 11, no. 1, pp. 89-106, 2024.

[8] M. Perez and R. Singh, "Vulnerability Detection in Medical IoT Systems Using Nessie: A Case Study," *Health Technology Journal*, vol. 6, no. 5, pp. 120-135, 2023.

[9] D. Kim and H. Park, "Practical Applications of Nessie for Basic Vulnerability Detection in Healthcare IoT," *Journal of Cybersecurity Practices*, vol. 9, no. 3, pp. 235-249, 2023.

[10] G. Zhang and N. Jafari Navimipour, "A Comprehensive and Systematic Review of the IoT-Based Medical Management Systems: Applications, Techniques, Trends and Open Issues," *Sustainable Cities and Society*, vol. 82, pp. 103914, 2022.

[11] S. Huda, M. R. Islam, J. Abawajy, V. N. Kottala, and S. Ahmad, "A Cyber Risk Assessment Approach to Federated

Identity Management Framework-Based Digital Healthcare System," *Sensors*, vol. 24, no. 16, pp. 5282, 2024.

[12] M. Adil, M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani, and Z. Jin, "Healthcare Internet of Things: Security Threats, Challenges and Future Research Directions," *IEEE Internet of Things Journal*, 2024.

[13] G. Carofiglio and S. Palazzo, "NS-3 Network Simulator for Next-Generation Wireless Networks," *IEEE Access*, vol. 8, pp. 34612-34621, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2969296

[14] A. Varga and R. Hornig, "An Overview of the OMNeT++ Simulation Environment," in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (Simutools)*, 2008, pp. 1-10. [Online]. Available: https://doi.org/10.4108/ICST.SIMUTOOLS2008.3027

[15] B. Lantz, B. Heller, and N. McKeown, "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, pp. 1-6. [Online]. Available: https://doi.org/10.1145/1868447.1868466

[16] IBM Security, "IBM X-Force Command Cyber Range: A Virtual Environment for Real-World Cybersecurity Training," 2018. [Online]. Available: https://www.ibm.com/security/xforce

[17] J. Ahrenholz, "Comparison of CORE Network Emulation Platforms," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2010, pp. 166-171. [Online]. Available: https://doi.org/10.1109/MILCOM.2010.5680217

[18] Cuckoo Sandbox, "Cuckoo Sandbox: Open Source Automated Malware Analysis," 2021. [Online]. Available: https://cuckoosandbox.org/

[19] Cisco Networking Academy, "Packet Tracer Instructor's Guide," 2019. [Online]. Available: https://www.netacad.com/courses/packet-tracer

[20] Rapid7, "Nexpose: Vulnerability Management Solution," 2021. [Online]. Available: https://www.rapid7.com/products/nexpose/

[21] P. Biondi and F. Desclaux, "Scapy: A Powerful Interactive Packet Manipulation Program," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC)*, 2004, pp. 371-380, doi: https://doi.org/10.1109/CSAC.2004.42.

[22] J. Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*, Syngress, 2007, available at https://www.syngress.com.

[23] A. O. Panhwar, A. A. Sathio, A. Lakhan, M. Umer, R. M. Mithiani, and S. Khan, "Plant health detection enabled CNN scheme in IoT network," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 344-335, 2022.

[24] A. A. Sathio, "A Study On The Conceptual Framework Of Data Warehousing In Health Sector In Pakistan: A Case Study of a Hospital System and Disease (Hepatitis C)," *International Journal of Computer (IJC)*, vol. 29, no. 1, pp. 59-81, 2018, available at https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1154.

[25] A. A. Sathio and A. M. Brohi, "The Imperative Role of Pervasive Data in Healthcare," in *Advances in Information Security*, M. S. Husain, M. H. B. Muhamad Adnan, M. Z. Khan, S. Shukla, and F. U. Khan, Eds., Springer, Cham, 2021, pp. 17-21, doi: https://doi.org/10.1007/978-3-030-77746-3_2.

[26] A. A. Sathio, M. A. Dootio, A. Lakhan, M. ur Rehman, A. O. Panhwar, and M. A. Sahito, "Pervasive Futuristic Healthcare and Blockchain Enabled Digital Identities - Challenges and Future Intentions," in *2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, IEEE, 2021, pp. 30-35.

[27] Z. A. Shaikh, A. A. Wagan, A. A. Laghari, K. Ali, M. A. Memon, and A. A. Sathio, "The Role of Software Configuration Management and Capability Maturity Model in System Quality," *IJCSNS*, vol. 19, no. 11, p. 114, 2019.

[28] R. Vavekanand, A. A. Sathio, V. Singh, and S. Anwar, "Water4.0: An Industrial Water Pollution Forecasting Using Machine Learning," 2024, available at SSRN 4849924.

[29] A. A. Sathio, S. A. Awan, A. O. Panhwar, A. M. Aamir, A. M. Brohi, and A. Burdi, "A Blockchain-Enabled Machine Learning Mask Detection Method for Prevention of Pandemic Diseases," *VAWKUM Transactions on Computer Sciences*, vol. 11, no. 1, pp. 165-183, 2023.

[30] A. A. Sathio, M. M. Rind, and A. Lakhan, "Deep Learning Algorithms and Architectures for Multimodal Data Analysis," in *Deep Learning for Multimedia Processing Applications*, CRC Press, 2024, pp. 74-113.

[31] V. Singh, A. A. Sathio, S. Anwar, R. Vavekanand, and R. Danish, "A Medical Imaging Approach for Recognising Mitral Regurgitation Through Machine Learning Methods in Cardiac Imaging," *Journal Name*, 2024.

[32] H. Shah, S. Ahmed, A. A. Sathio, and A. Burdi, "W-rank: A Keyphrase Extraction Method for Webpage Based on Linguistics and DOM-based Features," *VAWKUM Transactions on Computer Sciences*, vol. 11, no. 1, pp. 217-228, 2023.

[33] A. Ali, "Implementation of ETL Tool for Data Warehousing for Non-Hodgkin Lymphoma (NHL) Cancer in Public Sector, Pakistan," *LC International Journal of STEM*, vol. 2, no. 3, pp. 98-102, 2021, ISSN: 2708-7123.

[34] A. A. Sathio, M. M. Rind, and A. Lakhan, "Deep Learning Algorithms: Clustering and Classifications for Multimedia Data," in *Deep Learning for Multimedia Processing Applications*, CRC Press, 2024, pp. 114-145.

[35] I. Kotenko, I. Saenko, A. Privalov, and O. Lauta, "Ensuring SDN Resilience under the Influence of Cyber Attacks: Combining Methods of Topological Transformation of Stochastic Networks, Markov Processes, and Neural Networks," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 66, 2023, MDPI.

[36] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, "A survey on network simulators, emulators, and testbeds used for research and education," *Computer Networks*, vol. 237, p. 110054, 2023, Elsevier.

[37] S. H. Almotiri, M. Nadeem, M. A. Al Ghamdi, and R. A. Khan, "Analytic review of healthcare software by using quantum computing security techniques," *International Journal of Fuzzy Logic and Intelligent Systems*, vol. 23, no. 3, pp. 336-352, 2023, Korean Institute of Intelligent Systems.

[38] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395-9409, 2022, Elsevier.

[39] A. O. Panhwar, A. A. Sathio, N. M. Shah, and S. Memon, "A Scheme Based on Deep Learning for Fruit Classification," *Mehran University Research Journal of Engineering and Technology*, vol. 44, no. 1, pp. 8-19, 2025, Mehran University of Engineering & Technology, Jamshoro.