IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 30, No. 12, December, 2025, pp. 3131-3141
Journal homepage: http://iieta.org/journals/isi

An Integrated Threat Modeling and Mitigation Framework for IoT Healthcare Using MITRE ATT&CK and Cyber Kill Chain Models

Zineb Nadifi[1], Mariyam Ouaissa[1*], Mariya Ouaissa[2], Ali Kartit[1]

[1] Laboratory of Information Technologies, Chouaib Doukkali University, El Jadida 24000, Morocco
[2] Laboratory of Computer Science and Smart Systems, Cadi Ayyad University, Marrakech 40000, Morocco

Corresponding Author Email: ouaissa.mariyam@ucd.ac.ma

https://doi.org/10.18280/isi.301205

Received: 14 August 2025
Revised: 20 November 2025
Accepted: 16 December 2025
Available online: 31 December 2025

Keywords:
Internet of Medical Things, IoT healthcare security, MITRE ATT&CK mapping, Cyber Kill Chain analysis, threat modeling and mitigation, attack simulation, remote cardiac monitoring, adversary tactics and techniques

ABSTRACT

Healthcare systems are increasingly based on IoT architecture given their advantages it brings to the field, such as real-time monitoring of the patient's health status. However, the complexity of the IoT has increased the number of attack surfaces, jeopardising the security of confidential medical data. Some studies have highlighted the issues of security in IoT environments, but few have detailed the threats associated with the healthcare sector based on frameworks. This paper fills this gap by providing a comprehensive study in Internet of Medical Things (IoMT) using the MITRE ATT&CK matrix to identify and anticipate the techniques and tactics exploited by attackers against vulnerabilities in IoMT besides presenting a use case illustrating how attackers can endanger a patient's life by compromising a remote cardiac monitoring system following the Cyber Kill Chain. The study further highlights under-documented attack paths specific to healthcare IoT and proposes tailored technical and organizational mitigations. The novelty of this work lies in its integrated use of MITRE ATT&CK and the Cyber Kill Chain to put into perspective mapping of IoMT threats and a structured mitigation framework. This contribution provides a reference for security professionals to identify attack paths and build a model of security measures against cyber risk in IoMT.

1. INTRODUCTION

In recent years, an increasing number of sectors have embraced digital transformation to improve user interaction and ensure faster, more efficient service delivery. Domains such as banking, agriculture, commerce, and notably healthcare have all been impacted by this shift. Among these, healthcare stands out due to the sensitivity of the data it handles and the critical nature of its operations. Medical records, real-time patient monitoring, and time-critical interventions require not only speed but also accuracy and reliability [1].

In this context, the integration of Internet of Things (IoT) technologies opens new possibilities, enabling continuous patient care without the need for constant physical presence by healthcare professionals [2]. This is made possible with IoT architectures, which present a complete and structured ecosystem of interconnected devices and networks, ensuring a cycle designed to offer patients up-to-the-minute monitoring and treatment of their health status. Sometimes this occurs without the intervention of healthcare professionals such as doctors and nurses, since bodily and environmental signals are collected using sensors installed in patient rooms or worn by the patients themselves. These sensors record every change or stability depending on their nature, then send the data to gateways for primary analysis before being transmitted via the Internet to processing units based on AI and machine learning for in-depth analysis. These units return results showing the patient's current condition, sometimes even sending signals to adjust room parameters such as temperature, humidity, and ventilation, or issuing alerts for immediate medical intervention [3].

Admittedly, the healthcare field has benefited greatly from the facilities offered by IoT, which has significantly helped patients to be properly monitored and treated and has reduced the delay in urgent medical interventions, given the accuracy, speed, and efficiency of the analyses [4]. On the other hand, the transmission of such critical data across trusted and untrusted networks such as public networks and the Internet has increased cyber risks. This data can be compromised, affecting its confidentiality, or altered, putting its integrity at risk, or subjected to denial-of-service attacks against devices, servers, and sensors that affect their availability, as well as other risks such as identity theft, data encryption, and access blocking. The major problem here is that the consequences of these attacks can be serious, if not disastrous, given that they affect the health sector, which is constantly critical and sensitive, and that even a tiny change in its data can easily lead to catastrophic outcomes for patients or even an entire hospital or clinic [5].

Hence, cybersecurity experts are called upon to work proactively rather than reactively, to avoid threats and risks in advance by monitoring and complying with regulations and risk management standards, and by putting in place defense

and detection security measures. To meet the challenges posed by the use of IoT in healthcare, and to support proactive work, the MITRE ATT&CK framework has emerged as a structured and effective tool aimed at classifying Indicators of Compromise (IoCs) under a matrix with fourteen tactics and numerous techniques used by cybercriminals that define their behaviors and movements to compromise IT systems and devices. This helps cybersecurity experts understand and anticipate proactive and offensive actions [6].

This paper presents an analysis of the risks and threats of an IoT environment in the healthcare field, based on the tactics and techniques presented by MITRE ATT&CK. The structure of this paper is as follows: Section 2 provides an overview of previous works. Section 3 presents a description of healthcare in IoT environments. Section 4 provides an overview of the MITRE ATT&CK matrix, explaining its objective and usefulness for organizations and how to benefit from the knowledge base it offers. Section 5 is dedicated to threat modeling in this context, including a use case of an attack on a patient monitoring device, which is analyzed by deploying MITRE ATT&CK techniques in correlation with the Cyber Kill Chain. In Section 6, we present proposed mitigation and remediation solutions against the identified threats, along with a discussion. Finally, conclusions are drawn in Section 7.

2. RELATED WORK

Given the importance, timeliness, and richness of the topic, it has been extensively investigated in the literature through a wide range of studies and methodological approaches. The study by Zisad and Hasan [7] has analyzed the cyber risks associated with a healthcare system, specifically with Radiological Medical Devices (RMD), starting with a presentation of the RMD with the aim of discovering how it works, then defining the assets, and discovering the attackers' access points, which will help to build a Data Flow Diagram (DFD) representing an attacker model, and identify the vulnerabilities and threats present in the model, and propose mitigation strategies at the end to deal with these threats.

Li and Madisetti [8] also used the MITRE ATT&CK matrix to detect and prevent ransomware attacks on healthcare systems, by understanding the attackers' techniques and the IoCs that can be generated as the ransomware attack progresses, and using them to deduce mitigation solutions.

The paper by Abdelwahab et al. [9] used the MITRE ATT&CK framework to validate a robust defense system against attacks before they occur, which can help organizations minimize the damage and impact of security incidents. To do this, Abdelwahab et al. [9] first clarified a set of common terms such as vulnerability, risk, threat, etc. then cited specific examples of standards and norms of information security management that are essential for planning defense strategy, such as Critical Security Controls (CIS), and combined the MITRE ATT&CK tool and multi-criteria decision-making (MCDM) to propose a strong defense strategy.

Zahid et al. [10] conducted an in-depth analysis of the likely threats in the Industrial automation technologies domain, more specifically on the Cyber-Physical System (CPS) by mapping between MITRE ATT&CK, and NIST Security control framework to conclude that security controls are effective against identified threats, and which are known in the basis of the MITRE ATT&CK matrix.

Study by Jin et al. [11] presented the analysis of threats linked to IoT architectures, and chose to focus on the case of botnets whose aim is to carry out massive attacks on a target to impact its availability, and prevent it from responding when requested. Study by Jin et al. [11] begins by mentioning well-known botnet attacks, then describes MITRE ATT&CK, and the structure of the I3TM framework (Targeting-Threat Modeling) which will be deployed in the analysis of the attack chain by botnets on IoT architectures, by working on a concrete case of Medusa botnets.

This paper is a study of an IoT environment in the healthcare sector, clarifying the threats that can increase attack surfaces, identifying and evaluating them, using the MITRE ATT&CK framework, which was chosen because it gives a proactive view of the movements and actions of attackers according to their motivations, The paper presents a case study of the compromise of a remote cardiac patient monitoring system using the MITRE ATT&CK tool, and respecting the Cyber Kill Chain stages, and finally proposing mitigation solutions that greatly help to reduce attack surfaces and minimize risk, especially in a healthcare domain which operates with hyper-sensitive and critical data that can never tolerate the risks of compromise, unavailability, alteration or other.

3. HEALTHCARE IN IoT

IoT is an ecosystem of devices that are interconnected to create a network that can be managed, controlled and easily supervised remotely and sometimes without user interaction, but solely as a result of decisions taken based on AI analysis and machine learning. Many areas currently support an IoT architecture, such as the smart home, smart cities, e-commerce, vehicles and industry, and this is because the IoT has made a positive transformation in terms of user experience and ease of use, because it aims to keep environments in order and in line, and reduces human error and forgetfulness, as for example in the field of agriculture, fields can be watered when necessary, and in the way and quantity they need, by diagnosing and analyzing multiple factors such as humidity, drought, and temperature, using artificial intelligence, temperature and other environmental factors, which indicate the need to water them at the right moment, limiting human forgetfulness and misinterpretation, and optimizing the consumption of water resources.

As mentioned, the IoT is now present in various fields, including healthcare, which is the subject of this paper. The aim of this field is to take advantage of the services offered by the IoT so that healthcare professionals such as doctors and nurses can have information and data relating to their patients at any given moment, in order to supervise and control their state of health without needing to travel to their homes, or to relieve themselves of other tasks and stay with them in their homes, and at the same time while avoiding the risk of leaving them without medical supervision [12].

In order to ensure this network, there are a number of stages that need to link up, exchange and communicate with each other to build a chain that starts from the place where the patients are to the doctors, regardless of the location of these two parties [13].

- **Perception layer:** This is the layer that is in direct contact with patients via sensors that are either installed in their homes to measure humidity, temperature, etc., or portable sensors that collect, for example, heart rate, blood

pressure, blood sugar and the patient's heartbeat.

- **Network Layer:** The data collected beforehand will be transmitted to a gateway, which could be a smartphone, a dedicated gateway, etc., which initially pre-processes, analyses, aggregates and pre-processes the IoT data, translates the protocols and acts as a gateway between the IoT networks (e.g. ZigBee, Bluetooth, BLE) and the IP networks (Internet, cloud, CP/IP, MQTT, CoAP, LTE, 5G…depending on the range and bandwidth).
- **Processing Layer or Middleware Layer**: This is where data is processed, stored, filtered and analyzed, with the involvement of big data, AI, machine learning and database management in the cloud.
- **Application Layer:** This is the layer used for a man-machine interface with healthcare professionals via mobile applications, web portals and hospital software for teleconsultations, alerts, real-time monitoring, etc.
- **Security layer:** This is a transversal layer which ensures that security objectives - availability, integrity, confidentiality- are met and guaranteed by encryption, hashing, authentication, logging.

4. MITRE ATT&CK

MITRE ATT&CK is a commonly used paradigm for categorizing and documenting adversarial tactics, methods, and procedures. It assists security professionals in understanding, detecting, and responding to assaults by offering an organized matrix of typical attacker actions across multiple environments. This section describes the key components and primary versions.

4.1 Overview of MITRE ATT&CK

The term MITRE ATT&CK stands for MIT Research Establishment, while ATT&CK is an acronym for tactics, techniques and common adversary knowledge. It represents a tool presenting a structured and organized knowledge base in a matrix format of tactics and techniques adopted by adversaries and used by threat hunters, cyber defense professionals, and red teams to better understand attackers' strategy and approach, their behaviors, classifying them and analyzing attack lifecycle stages and common adversary behaviors, so that they can understand attacker tactics in advance, and anticipate a hunt using the framework, tactics are mapped to techniques, which are further broken down into sub-techniques [14].

MITRE ATT&CK is available in various versions and matrices, each suitable for a specific technical environment. The most commonly used are listed below [15].

- **MITRE ATT&CK for Enterprise**

Used very often in traditional IT environments and supports different systems such as Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, AWS, GCP...etc which makes this version more sought after by SOC teams, and in security audits and IS hardening [16].

- **MITRE ATT&CK for Mobile**

It is a version that supports attacks targeting smartphones and tablets using Android or iOS systems, and is in greater demand in the case of BYOD security and mobile medical applications [17].

- **MITRE ATT&CK for Industrial Control Systems (ICS)**

Dedicated to industrial systems (SCADA, PLCs, RTUs, HMI, etc.), very often applied with great criticality in the OT (Operational Technology) domain as in energy, health, and production [18].

- **MITRE ATT&CK for Cloud**

Is a sub-category of the Enterprise matrix; but which takes into consideration techniques dedicated to the cloud, it is used for public cloud services (AWS, Azure, GCP, etc.), and ensures cloud security, SaaS, IaaS...

4.2 Tactics, techniques, and sub-techniques

The tactics present the motivation and rationale of the attackers, the techniques describe how the attackers achieved their goals, the sub-techniques provide a higher level of precision than the techniques, by describing exactly how the technique was deployed by the attacker. The following are examples of the tactics used by MITRE ATT&CK for each version [19].

- **MITRE ATT&CK for Enterprise**

- Exfiltration (TA0010): Removing and stealing data from the target machine.

- Execution (TA0002): Launching malicious code on the target's system.

- Command and Control (TA0011): Communicating with the target remotely in order to gain control.

- **MITRE ATT&CK for Mobile**

- Initial Access (TA0027): Obtaining an entry point that serves as a first access to the mobile.

- Persistence (TA0028): Establishing a lasting presence and access even after the target has been rebooted, updated, or cleaned.

- Impact (TA0034): Affect the target by destroying it, encrypting it, disrupting its operation, etc.

- **MITRE ATT&CK for ICS (Industrial Control Systems)**

- Impair Process Control (TA0115): Aiming to collect and use a set of techniques and methods to cause disruption and malfunction of an industrial process, impact its production, disrupt its safety...

- Inhibit Response Function (TA0114): Techniques used by the adversary to hinder or disable security functions altogether.

- Collection (TA0100): Gather data useful for achieving your objective, such as documents, from the ICS environment.

- **MITRE ATT&CK for Cloud**

- Reconnaissance (TA0043): Gathering information about the target that can be used to carry out an attack (example: cloud buckets).

-Resource Development (TA0042): Preparing and establishing the resources, tools and access needed to carry out the attack like malicious cloud accounts.

- Defense Evasion (TA0005): Bypassing and hiding the actions and movements of security tools in the cloud environment so as not to detect the attacker's malicious presence.

The techniques and sub-techniques are numerous. Table 1 showing some examples for each version of the MITRE ATT&CK matrices.

Table 1. Overview of MITRE ATT&CK tactics, techniques, and example sub-techniques

Tactic	Technique Reference	Technique	Technique Description	Sub-technique Reference	Sub-technique	Sub-technique Description
MITRE ATT&CK for Enterprise						
Execution	T1059	Command and Scripting Interpreter	Execution of commands via interpreters.	T1059.001	PowerShell	Execution of malicious scripts using PowerShell.
Defense Evasion	T1027	Obfuscated Files or Information	Use obfuscation to hide malicious code or files.	T1027.002	Software Packing	Use of packers to compress or encrypt executables.
Credential Access	T1003	OS Credential Dumping	Extraction of passwords or hashes from the system.	T1003.001	LSASS Memory	Dumping credentials from LSASS memory.
MITRE ATT&CK for Mobile						
Persistence	T1406	Obtain Device Administrator Permissions	Gain control by acquiring device admin permissions.	T1406.001	Device Admin Access	Using admin rights to maintain access.
Credential Access	T1414	Input Capture	Capture user inputs such as passwords or messages.	T1414.001	Keylogging	Logging keystrokes entered by the user.
Impact	T1471	Data Encrypted for Impact	Encrypt data to render it unavailable.	T1471.001	App Data Encryption	Encrypt application data to cause impact.
MITRE ATT&CK for ICS (Industrial Control Systems)						
Impair Process Control	T0830	Manipulate Control Logic	Altering device logic to disrupt processes.	T0830.001	Modify Program	Modifying logic in the PLC or controller.
Inhibit Response Function	T0814	Alarm Suppression	Disabling alarms to avoid detection.	T0814.001	Suppress Safety Alarms	Preventing safety alerts from being triggered.
Collection	T0802	Data from Information Repositories	Access stored logs or configs.	T0802.001	PLC Logs	Collecting logs from programmable logic controllers.
MITRE ATT&CK for Cloud						
Discovery	T1087.004	Cloud Account Discovery	Identify cloud accounts and privileges.	T1087.004	IAM Users	Listing IAM users in cloud environments.
Resource Development	T1583.003	Virtual Private Server	Use of VPS for staging attacks.	T1583.003	Cloud VPS	Renting cloud servers for malicious use.
Impact	T1499.004	Cloud Service Denial	Disrupt cloud service availability.	T1499.004	Serverless Function Abuse	Trigger excessive execution to exhaust resources.

5. PROPOSED METHODOLOGY

In this study, a threat modelling methodology will be proposed that is inspired by generic threat modelling models but projected onto an Internet of Medical Things (IoMT) environment, not only to follow the traditional steps but also to extract concrete outputs and artefacts that will form the basis of a threat and risk classification analysis in the IoMT. These will then be used in the construction of a classification framework for threats and risks in the IoMT. but also to extract concrete outputs and artefacts that will form the basis of a threat and risk classification analysis in the IoMT, and which will thus be used in constructing the attack path discussed in section 6.

Threat modelling generally begins with a design phase, which involves capturing the requirements of the system in question and developing a flow diagram. The detection phase then consists of applying a threat modelling framework to the flow diagram in order to identify existing security issues, which leads to the correction stage, which aims to correct vulnerabilities. and finally, the verification phase, which ensures that the corrections have been properly applied and are now operational. This generic model will be the reference in this paper in order to build and propose a model that meets the requirements and constraints of an IoMT environment and aims to generate a formal artefact used later in the Results section. This model consists of four phases:

5.1 Assets identification

This first step involves extracting an inventory of assets in the IoMT, which will then be used in section 6.1 to map the threats to specific assets. The result is a structured asset catalogue divided into:

- **Hardware assets**

- Sensors: portable and non-portable sensors such as connected insulin pumps, ECGs, oximeters, glucometers, etc.

- Telephones and smartphones: used by healthcare professionals to monitor and assist patients.

- IoT environment equipment: such as routers, gateways, servers, access points, etc.

Software assets

- Mobile applications: used by healthcare professionals and patients for monitoring purposes.

- Operating systems: the operating systems installed on all equipment to make it work.
- Cloud platforms: AWS IoT, Azure IoT Hub, Google Cloud Healthcare

- **Information assets**

- Personal data: of healthcare staff and patients, including names, surnames, telephone numbers, etc.
- Patient health information: their diagnoses, blood types, medical history, etc.
- Healthcare professional accounts: credentials they use to access mobile applications, mobile phones and workstations.
- Network traffic: exchanges and information circulating between devices.
- Equipment configurations: configuration files embedded in equipment to enable it to perform its tasks.
- Logs: logs recorded in monitoring tools.

- **Commercial assets**

- The reputation of the hospital/clinic.
- The image of healthcare professionals.

- **Human assets**

- Healthcare professionals: doctors, nurses, laboratory technicians, etc.
- IT administrators: experts responsible for managing applications, platforms and equipment maintenance.
- Patients: users wearing sensors and monitored by doctors.

5.2 Data flow diagram

The data flow diagram (DFD) is divided into three areas: the patient area, where the patient is located and where sensors are placed either in the environment to detect temperature, air, etc., or in the patient's body to measure various health-related parameters, such as respiratory rate, blood sugar, etc., i.e. the area in direct contact with the patient; the processing area, very often in the cloud, is the area where all the collected data will be stored and processed immediately or for later analysis; and the healthcare and professional area, where doctors, nurses and healthcare technicians are located, who receive updates on the health status of their patients and can instantly adjust any parameters that need to be regulated [20]. This provides them with dashboards and reports that summarize the patient's average condition on a daily, weekly, monthly, etc. basis. The DFD in Figure 1 shows a diagram of the three areas mentioned, indicating the traffic flowing between them and ensuring that remote monitoring is maintained via an IoT network [21, 22].

The DFD therefore constitutes the attack surface model as a second result, enabling the systematic extraction of threats. Section 6 uses this DFD to justify the attack paths and the Kill Chain scenario.

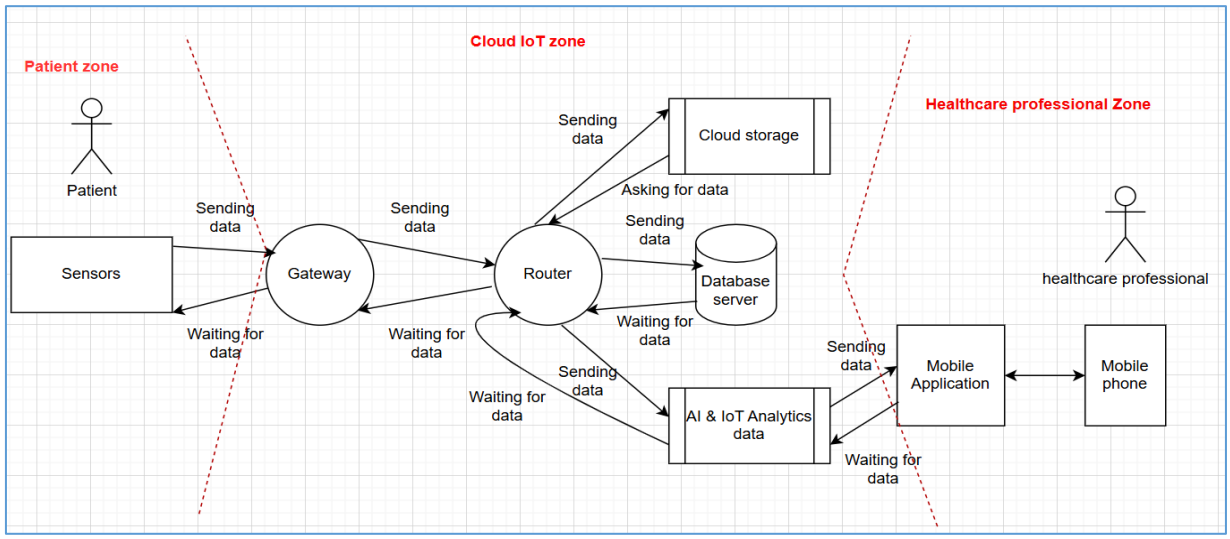

Figure 1. Data flow diagram of healthcare in IoT environment

5.3 Threat identification

Threat identification is a crucial phase of this threat modelling methodology as a third outcome, particularly in the IoMT environment, which involves the processing of highly critical and sensitive information, such as healthcare. Using the catalogue of assets identified in section 5.1 and the DFD developed in section 5.2, a formal threat model can be generated and composed of the following elements:

- Potential threat agents (external cybercriminals, malicious insiders, compromised IoT devices, supply chain attackers).
- A list of threat events affecting each asset,
- Their mapping to compromised security objectives (CIA).
- Impacted asset
- MITRE ATT&CK technique
- MITRE ATT&CK matrix

Section 6.1 directly reuses this model to map each threat to MITRE ATT&CK techniques.

5.4 Threat mitigation

Each threat present in the IoMT environment leads to a risk of varying levels of criticality based on two main factors, Likelihood (L) and Impact (I): assessed as Low, Medium, or High, the combination of these two parameters on IoMT threats generates the fourth output, which is the risk matrix presented in a table in section 6.2.

5.5 Generic IoMT attack model

Section 6.3 details the path of an attack model in an IoMT environment aimed at compromising remote cardiac monitoring following the steps of the Cyber Kill Chain model; but in general, attackers very often target the following elements in order to breach IoMT security, which will be counted as the fifth output -generic attack model:

- Compromise of sensing device.

- Gateway compromise.
- Cloud service exploitation.
- Clinicien application manipulation.

The first output, Asset catalogue, from section 5.1 Asset identification will be used in section 6.1, while the second output, Attack surface model, extracted from section 5.2 DFD creation will be used in both sections 6.1 and 6.2. The third output, Formal threat model, which we were able to extract from the Threat identification stage, will be useful in section 6.1 and for formulating Table 2. The produced output Risk Matrix from the Risk assessment stage and the Generic adversarial flow generated from the IoMT attack model stage will be the input and input data for formulating the attack path following the Cyber Kill Chain method, section 6.3 demonstrates how this model specializes in the cardiac monitoring Kill Chain.

6. RESULTS AND DISCUSSION

The results presented in this section are the direct application of the methodology developed in Section 5. Each methodological artefact, asset catalogue, threat model, risk matrix, ATT&CK mapping, and attack model is projected onto the IoMT use case. We then propose mitigation techniques to strengthen the security of smart healthcare against potential attacks.

6.1 Application of the threat model to IoMT assets

Given that the IoMT architecture is complex and heterogeneous, using a single version of MITRE ATT&CK such as Enterprise will be insufficient to cover all the techniques used by attackers in such an environment, and demonstrates a limitation in terms of the compatibility of IoMT components, each of which belongs to a distinct operational environment. Although portable medical sensors communicate using BLE/ZigBee, which will be aligned with MITRE Mobile, gateways (patients' smartphones) function as conventional IT systems running on Android/iOS, aligned with MITRE Mobile/ Enterprise, cloud-based analytics platforms (FHIR API, IoT Hub ingestion, dashboards) will be aligned with MITRE Cloud, and embedded medical devices with real-time logic (ECG firmware, actuators, telemetry pipelines) behave similarly to ICS environments due to their deterministic control logic and critical safety constraints, so calling on multiple versions of MITRE ATT&CK is not a plus; rather, it is a necessity and an obligation. This mixed matrix approach is therefore aligned with recommendations from recent research on IoMT and avoids oversimplification.

Based on the asset catalogue and DFD presented in sections 5.1 and 5.2, threats were mapped to the relevant assets and associated with MITRE ATT&CK techniques. This resulted in the mapping of threats, assets and techniques presented in Table 2. This step converts the methodological threat model into operational information.

6.2 Risk matrix table

The risk matrix based on Likelihood and Impact levels is applied below to the threats listed in section 6.1 in Table 2. The risk matrix helps to prioritize risks according to their criticality and decide which ones to select for the Kill Chain reconstruction (Table 3).

6.3 Use case: Compromise of a remote cardiac patient monitoring system, Cyber Kill Chain analysis

To ensure a clear alignment between the methodological outputs (Section 5) and the applied analysis (Section 6), this use-case scenario integrates the results of the risk assessment presented in the Risk Matrix (Table 3). Only threats assessed as High or Critical were selected to construct the attack path, meaning that the Kill Chain focuses on the most dangerous and plausible adversarial actions within an IoMT cardiac-monitoring environment (Table 4 and Figure 2) [23, 24]. Accordingly, the following threats from the matrix directly drive the construction of the attack scenario:

Critical: exploitation of device vulnerabilities, data exfiltration, ransomware, account theft

High: firmware modification, supply-chain compromise, APT intrusion, phishing

Reconnaissance: Targeting the ECG sensor and gateway (Critical)

The first step in the Cyber Kill Chain is to collect publicly exposed vulnerabilities in cardiac monitoring devices, such as leaked vendor documentation, mobile application metadata, and others, by following the ECG communication path via Bluetooth Low Energy (BLE), which transfers data to a smartphone acting as a gateway using MQTT over TLS.

The most relevant MITRE ATT&CK techniques that can be used during this phase are as follows:

- T1592: Collect information about the victim host (reverse engineering mobile applications)
- T1595: Active scanning (BLE enumeration)
- T1597: Search for closed sources

Weaponization: Creation of exploits for firmware and BLE (High)

From the reverse-engineered firmware, the attacker prepares a maliciously modified ECG firmware capable of causing noise in the ECG waveform, thus bypassing integrity checks. To do this, the following two tactics can be used:

- T1608.004: Phase Capabilities: Target on Passage (the attacker prepares their weapon to infect weak firmware).
- T1552.001: Insecure Credentials: Credentials in Files (extraction of hard-coded AES keys used for BLE pairing).

Delivery: BLE-based injection and supply chain abuse (High)

In order to deliver the modified malicious ECG firmware, the attacker can take one of two routes: BLE Over-the-Air (OTA) local update spoofing or compromised third-party cloud component, which justifies the use of the following three techniques:

- T1195: Supply chain compromise
- T1412: SMS message capture (abuse of BLE pairing weaknesses)
- T1476: Malicious application delivery (trojanised patient gateway application)

Exploitation: Privilege escalation on the gateway (Critical)

Once the trojanied patient application has been delivered, the attacker exploits a privilege escalation vulnerability in Android's BLE service management, as well as weak authentication on the MQTT broker used by the gateway, leading to the use of the following techniques:

- T1068: Exploitation for privilege escalation
- T1531: Account access suppression (disabling legitimate alerts on the application)
- T1556: Modification of the authentication process (alteration of MQTT token generation)

Installation: Stealthy persistence inside the sensor (Critical)

The malicious firmware implants a secret C2 channel using unused BLE characteristic values and a hidden task inside the RTOS to reinfect the legitimate firmware using:
- T1542.004: Pre-boot operating system: ROMMONkit
- T1037.005: Startup or login initialization scripts: startup elements

Command and control: Secret signaling via MQTT (Critical)

Instead of the classic HTTP-based C2, the attacker uses MQTT message fields to send encoded commands such as malformed QoS bits, which corresponds to an uncommon attack technique from MITRE ATT&CK:
- T1071.004: Application Layer Protocol: MQTT
- T1573: Encrypted Channel
- T1205: Traffic Signaling

Objectives: Data Manipulation and Alert Suppression (Critical)

The attacker performs IoMT-specific malicious actions, such as manipulating the ECG signal via T0831: Manipulation of control (ICS adapted to the medical analysis pipeline), and suppression of alerts so that real-time alerts do not reach cardiologists via TA0107: Inhibition of the response function, and exfiltration of medical data such as patient identifiers via normal MQTT telemetry via T1041: Exfiltration via the C2 channel.

Table 2. IoT healthcare threat classification using MITRE ATT&CK framework

Threat Event	Asset Impacted	Threat Agent	CIA Impact	MITRE ATT&CK Technique	Justification of Matrix Version
Installation of a malicious healthcare mobile app	Patient smartphone / Mobile health app	External cybercriminal	C, I	Malicious App (T1476)	Mobile (smartphone gateway is mobile OS)
Exploitation of vulnerabilities in IoT medical devices	Wearable sensors / Home sensors / Gateways	External attacker / Compromised IoT bot	C, I, A	Exploit Public-Facing Application (T1190), Valid Accounts (T1078), Brute Force (T1110)	Enterprise + Mobile (gateway = Enterprise logic + wireless pairing = Mobile)
Phishing targeting healthcare staff	Clinician workstation / Email service / Mobile	External cybercriminal	C	Phishing (T1566)	Enterprise (staff workstations, hospital email)
Modification of sensor or medical device firmware	Medical sensors / IoMT embedded device firmware	Supply-chain attacker / Advanced threat actor	I, A	System Firmware (T0857), Pre-OS Boot: ROMMONkit (T1542.004)	ICS (real-time control logic similar to ICS)
Theft and exfiltration of sensitive patient data	Cloud storage / Databases / Gateways	External attacker	C	Credential Dumping (T1003), Exfiltration Over C2 Channel (T1041), Data from Information Repositories (T1213)	Cloud + Enterprise (Data can be stored in the cloud, hence the cloud version, or in transit in the gateway and network, hence the enterprise version.)
IoT botnet attack disrupting device availability	IoT sensors / Gateways / Network	Compromised IoT bot / Remote attacker	A	Acquire Infrastructure (T1583), Ingress Tool Transfer (T1105), Network Service Discovery (T1046)	Enterprise (botnet malware operations occur at network layer)
Targeted APT attack against healthcare infrastructure	Cloud backend / Hospital network	APT group	C, I, A	Reconnaissance (TA0043), Persistence (TA0003), Privilege Escalation (TA0004), Defense Evasion (TA0005)	Enterprise + Cloud (privileged admin accounts + cloud APIs)
Ransomware impacting patient data and clinical services	Cloud servers / Clinician workstation / Databases	Cybercriminal group	A, C	Data Encrypted for Impact (T1486), Data Destruction (T1485), Endpoint Denial of Service (T1499)	Enterprise (Ransomware affects enterprise systems and data)
IoT healthcare supply-chain compromise	Firmware updates / Third-party components	Supply-chain adversary	I, A	Trusted Relationship (T1199)	Enterprise (supplier compromise)
Theft of healthcare professional accounts	Clinician account / IAM / Application session	Malicious insider / External attacker	C, I	Valid Accounts (T1078), Modify Authentication Process (T1556), OS Credential Dumping (T1003)	Enterprise

Table 3. Risk matrix table

Threat	Likelihood	Impact	Risk Level
Installation of a malicious healthcare mobile app	Medium	Medium	**Medium**
Exploitation of vulnerabilities in IoT medical devices	High	High	**Critical**
Phishing targeting healthcare staff	High	Medium	**High**
Modification of sensor or medical device firmware	Medium	High	**High**
Theft and exfiltration of sensitive patient data	High	High	**Critical**
IoT botnet attack disrupting device availability	Medium	Medium	**Medium**
Targeted APT attack against healthcare infrastructure	Medium	High	**High**
Ransomware impacting patient data and clinical services	High	High	**Critical**
IoT healthcare supply-chain compromise	Medium	High	**High**
Theft of healthcare professional accounts	High	High	**Critical**

Table 4. Mapping of risk-prioritized threats to Kill Chain stages and ATT&CK techniques

Kill Chain Stage	High/Critical Threat (from Risk Matrix)	Examples of ATT&CK Techniques
Reconnaissance	Exploitation of IoMT device vulnerabilities (Critical)	T1592, T1595
Weaponization	Firmware modification (High)	T1608.004, T1552.001
Delivery	Supply-chain compromise (High)	T1195, T1476
Exploitation	Account theft / privilege abuse (Critical)	T1068, T1556
Installation	Persistence through firmware (High)	T1542.004, T1037.005
Command & Control	Data exfiltration via covert MQTT (Critical)	T1071.004, T1573
Actions on Objectives	Data theft, service disruption (Critical)	T0831, T1041

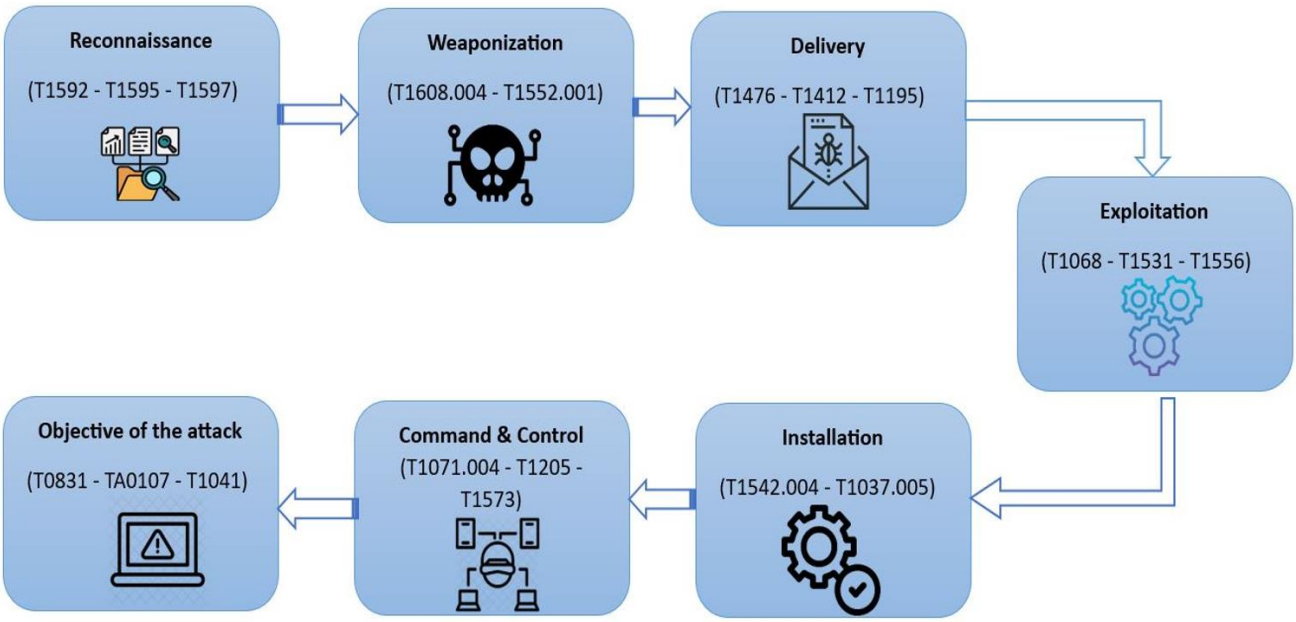

Figure 2. Diagram of Kill Chain stages of compromise of patient system correlated with MITRE ATT&CK

6.4 Countermeasures and mitigation mechanisms

In order to correct the potential threats previously identified in Table 2, the following solutions are proposed:

a- Installation of a Malicious Healthcare Mobile App

- Mandatory verification of digital signatures for healthcare applications (M1016: Code Signing).
- Deployment of an MDM to control installations (M1003: Application Vetting).
- Raising patient awareness of the risks of unofficial APKs (M1017: User Training).
- Enforcing installation via official stores using an 'allowlist' (M1002: Platform Security).
- Strengthening Android/iOS permissions to limit privilege escalation (M1018: OS Security Configuration).

b- Exploitation of Vulnerabilities in IoT Medical Devices

- Patches and firmware updates, with integrity verification (M1051: Update Software).
- Removal of default identifiers, regular key rotation (M1027: Password Policies).
- Strict network segmentation (dedicated medical VLANs) to limit lateral movement (M1030: Network Segmentation).
- Enable mutual TLS for sensors/gateways (M1041: Encrypt Network Traffic).
- Implement minimal exposure surface: disable unnecessary services (M1042: Disable Unnecessary Features).

c- Phishing Targeting Healthcare Staff

- Regular phishing simulation campaigns (M1017: User Training).
- Enable MFA on healthcare accounts (M1032: Multi-Factor Authentication).
- Deployment of anti-spam filters and DLP (M1021: Restrict Web-based Content).

- Behavioral analysis of accounts via UEBA (User Behavior Analytics).
- Blocking of dangerous macros and attachments (M1047: Audit).

d- Modification of Sensor or Medical Device Firmware

- Mandatory digital signature for all firmware (M1016: Code Signing).
- Startup integrity attestation process (Secure Boot) (M1046).
- Disabling of unsecured debug/OTA ports (M1042).
- Inventory and strict control of deployed firmware versions (M1013: Application Inventory).
- Enhanced physical security of devices (tamper-proofing) (M1050).

e- Theft and Exfiltration of Sensitive Patient Data

- Encryption of data at rest, in transit and in RAM (M1041).
- Least Privilege Access and Zero Trust to limit data exposure (M1026).
- Monitoring of outgoing traffic (DLP + L7 firewall) (M1037: Filter Network Traffic).
- Detection of anomalies in IoMT/MQTT traffic (M1031: Network Intrusion Prevention).
- Segmentation of patient data in segmented cloud environments (M1030).

f- IoT Botnet Attack Disrupting Device Availability

- IoT-aware IDS/IPS to detect botnet behavior (M1031).
- Segment critical devices in isolated medical VLANs.
- Regularly update vulnerable components (M1051).
- Rate-limit cloud endpoints to block saturation (M1030).
- Block communications to C2 via Threat Intelligence Feeds (M1035: Limit Access to C2).

g- Targeted APT Attack Against Healthcare Infrastructure

- Deployment of SIEM, EDR, and NDR for complete visibility (M1036: Monitoring).
- Zero Trust architecture (continuous verification) (M1026).
- Frequent key rotation, strict management of privileged accounts (M1027: Password Policies).
- Segmentation of critical infrastructure (DMZ, FHIR API, data lakes).
- APT response plan with continuous threat hunting (M1035).

h- Ransomware Impacting Patient Data & Clinical Services

- Behavioral detection of abnormal encryption (M1040: Behavioral Analytics).
- Offline backups, tested and restorable (M1053: Data Backup).
- Automatic isolation of suspicious hosts (M1030: Segmentation).
- Rigorous application of patches (M1051).
- Enhanced access control and MFA (M1032).

i- IoT Healthcare Supply Chain Compromised

- Verification of suppliers according to ISO 27001, ISO 13485, FDA cybersecurity guidance.
- SBOM (Software Bill of Materials) analysis for each component (M1051).
- Control of third-party libraries before deployment (M1047).
- Detection of code modifications, signatures and hashes (M1016).
- Rapid isolation of compromised components (M1030).

j- Theft of Healthcare Professional Accounts

- Mandatory MFA (M1032).
- Continuous auditing of accounts and rights (M1018: Account Use Policies).
- Regular rotation of passwords/keys (M1027).
- Detection of abnormal usage via UEBA (M1040).
- Passkeys and strong authentication for cloud access.

6.5 Discussion

Threat modelling can be carried out using different approaches and tools. In this study, MITRE ATT&CK was chosen and projected into an IoT environment in the healthcare sector. The application of the matrix revealed significant and rich results regarding the threats that may arise in the IoMT environment, and systematically revealed vulnerabilities that can be targeted by attackers who very often target this domain given the sensitivity and criticality of the data processed and circulated in this network. MITRE ATT&CK clarified a set of techniques used by attackers according to their motivations, which are presented as tactics in the framework. For example, T1566 in Table 2 presents the phishing technique exploited by the attacker to gain initial access to the target, which is presented by the 'Initial Access' tactic in MITRE ATT&CK. The phishing technique can be executed with one of the sub-techniques T1566.001 Spearphishing Attachment, T1566. 002 Spearphishing Link, T1566.003 Spearphishing via Service, and T1566.004 Spearphishing Voice, depending on the targeted victim. According to MITRE ATT&CK, the attacker can also guarantee the 'Initial Access' tactic through the Trusted Relationship technique (T1199) by compromising a third party or trusted entity in direct interaction with the target. T1041, presenting Exfiltration Over C2 Channel, is a technique identified by the attacker when their motivation/technique is 'Exfiltration' or data theft by exfiltration via a Command-and-Control channel. To better understand threats through MITRE ATT&CK techniques, this paper discusses a use case study that traces the path of an attack following the Cyber Kill Chain cycle, which consists of seven stages. Each stage has been correlated with a MITRE ATT&CK technique that meets the requirements for completing the stage in question. This study helps to better identify threats affecting healthcare in an IoT domain. Effective identification with MITRE ATT&CK and Cyber Kill Chain paves the way for correction and mitigation, as MITRE ATT&CK extracts tactics, techniques, and sub-techniques by putting on the hat of an attacker, which facilitates their detection and reduces the attack surface.

7. CONCLUSION

This paper addressed healthcare threats in an IoT environment based on the MITRE ATT&CK framework, which helps identify attackers' tactics and techniques in order to anticipate their movements and actions in the environment. The MITRE ATT&CK matrix was used in its officially published versions (Enterprise, Mobile, ICS, and, where applicable, Cloud), selected according to the components and attack surfaces relevant to the IoMT use case. The use of MITRE ATT&CK contributed positively to the proposal of mitigation and correction measures for the identified threats. In conclusion, this study enabled a detailed and in-depth analysis of threats that may arise in an IoMT environment by leveraging the different existing ATT&CK matrices:

Enterprise for network and application-level behaviors, ICS for device-level and firmware-related threats, Cloud for backend platforms, and Mobile for systems involving smartphones and BLE-based interactions. Regarding future work, ongoing discussions within the MITRE community indicate an interest in developing healthcare-tailored ATT&CK mappings; however, no official domain-specific ATT&CK version for healthcare has been released at the time of writing. Once such an official version becomes available, it may further facilitate and optimize threat identification, management, and mitigation in IoMT environments.

REFERENCES

[1] Nadifi, Z., Ouaissa, M., Ouaissa, M., Kartit, A., Kaushik, K., Choudhury, A. (2025). Mitigating phishing attack in IoT based healthcare system using a threat modeling approach. In 2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, pp. 933-938. https://doi.org/10.1109/InCACCT65424.2025.11011350

[2] Ramachandraiah, K.R.D., Bommagani, N.J., Jayapal, P.K. (2023). Enhancing healthcare data security in IoT environments using blockchain and DCGRU with twofish encryption. Information Dynamics and Applications, 2(4): 173-185. https://doi.org/10.56578/ida020402

[3] Kumar, N. (2017). IoT architecture and system design for healthcare systems. In 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bengaluru, India, pp. 1118-1123. https://doi.org/10.1109/SmartTechCon.2017.8358543

[4] Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future internet, 12(9): 157. https://doi.org/10.3390/fi12090157

[5] Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F., Yongchareon, S. (2024). Health IoT threats: Survey of risks and vulnerabilities. Future Internet, 16(11): 389. https://doi.org/10.3390/fi16110389

[6] Al-Sada, B., Sadighian, A., Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. ACM Computing Surveys, 57(1): 1-37. https://doi.org/10.1145/3687300

[7] Zisad, S.N., Hasan, R. (2024). Towards a security analysis of radiological medical devices using the MITRE ATT&CK Framework. In SoutheastCon 2024, pp. 1577-1582. https://doi.org/10.1109/SoutheastCon52093.2024.10500224

[8] Li, X., Madisetti, V.K. (2024). ERAD: Enhanced ransomware attack defense system for healthcare organizations. Journal of Software Engineering and Applications, 17(5): 270-296. https://doi.org/10.4236/jsea.2024.175016

[9] Abdelwahab, I., Hefny, H.A., Darwish, N.R. (2024). Enhancing cybersecurity defenses: A multicriteria decision-making approach to MITRE ATT&Ck Mitigation strategye. Available at SSRN 4907361. https://doi.org/10.2139/ssrn.4907361

[10] Zahid, S., Mazhar, M.S., Abbas, S.G., Hanif, Z., Hina, S., Shah, G.A. (2023). Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. Internet of Things, 22: 100766. https://doi.org/10.1016/j.iot.2023.100766

[11] Jin, H., Jeon, G., Choi, H.W.A., Jeon, S., Seo, J.T. (2024). A threat modeling framework for IoT-Based botnet attacks. Heliyon, 10(20): e39192. https://doi.org/10.1016/j.heliyon.2024.e39192

[12] Naresh, V.S., Pericherla, S.S., Murty, P.S.R., Reddi, S. (2020). Internet of Things in Healthcare: Architecture, applications, challenges, and solutions. Computer Systems Science & Engineering, 35(6). https://doi.org/10.32604/csse.2020.35.411

[13] Selvaraj, S., Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: A systematic review. SN Applied Sciences, 2(1): 139. https://doi.org/10.1007/s42452-019-1925-y

[14] Georgiadou, A., Mouzakitis, S., Askounis, D. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. Sensors, 21(9): 3267. https://doi.org/10.3390/s21093267

[15] Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., Chanakya, G. (2022). Analysis of cyber threat detection and emulation using MITRE attack framework. In 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), San Antonio, TX, USA, pp. 4-12. https://doi.org/10.1109/IDSTA55301.2022.9923170

[16] Branescu, I., Grigorescu, O., Dascalu, M. (2024). Automated mapping of common vulnerabilities and exposures to MITRE ATT&CK tactics. Information, 15(4): 214. https://doi.org/10.3390/info15040214

[17] Younis, A.A., Daher, Z., Martin, B., Morgan, C. (2022). Mapping zero-click attack behavior into MITRE ATT&CK mobile: A systematic process. In 2022 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 890-896. https://doi.org/10.1109/CSCI58124.2022.00160

[18] Choi, W., Pandey, S., Kim, J. (2024). Detecting cybersecurity threats for industrial control systems using machine learning. IEEE Access, 12: 153550-153563. https://doi.org/10.1109/ACCESS.2024.3478830

[19] Al-Sada, B., Sadighian, A., Oligeri, G. (2023). Analysis and characterization of cyber threats leveraging the MITRE ATT&CK database. IEEE Access, 12: 1217-1234. https://doi.org/10.1109/ACCESS.2023.3344680

[20] Das, P., Asif, M.R.A., Jahan, S., Ahmed, K., Bui, F.M., Khondoker, R. (2024). STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. Vehicles, 6(3): 1140-1163. https://doi.org/10.3390/vehicles6030054

[21] Xiong, W., Lagerström, R. (2019). Threat modeling–A systematic literature review. Computers & Security, 84: 53-69. https://doi.org/10.1016/j.cose.2019.03.010

[22] Nadifi, Z., Ouaissa, M., Ouaissa, M., Alhyan, M., Kartit, A. (2025). STRIDE-based threat modeling and risk assessment framework for IoT-enabled smart healthcare systems. International Journal of Online and Biomedical Engineering (iJOE), 21(9): 63-80. https://doi.org/10.3991/ijoe.v21i09.55517

[23] Zhao, L. (2024). Navigating the Cyber Kill Chain: A modern approach to pentesting. Applied and Computational Engineering, 38: 170-175. https://doi.org/10.54254/2755-2721/38/20230549

[24] Fadzil, L.M., Manickam, S., Al-Shareeda, M.A. (2023).

A review of an emerging Cyber Kill Chain threat model. In 2023 Second International Conference on Advanced Computer Applications (ACA), Misan, Iraq, pp. 157-161. https://doi.org/10.1109/ACA57612.2023.10346959