A FRAMEWORK FOR DEVELOPING SECURE INTERNET OF MEDICAL THINGS: A COMPREHENSIVE ROADMAP FROM AN ARTIFICIAL INTELLIGENCE PERSPECTIVE

BANDAR M. ALSHAMMARI
College of Computer and Information Sciences
Jouf University, Saudi Arabia
E-mail: bmshammeri@ju.edu.sa

ABSTRACT

The Internet of Medical Things (IoMT) has gained an extensive reputation in many applications within medical sectors. The late expansion of using these technologies has helped many organizations to progress well by delivering high-quality services. Such advancements and developments wouldn't hide the fact that such technologies also have many risks associated with their usage. Such risks vary in their severity depending on many factors, including the type of services IoMT provides and the customers it serves. However, the most important risks these systems are lately facing are related to their security. Therefore, any IoMT has to be secure enough in order to gain the trust and credibility of its clients. Although the IoMT security issues have been considered in several studies, enough attention has not been given to the best practices for developing secure applications. In fact, not following a precise and well-structured framework for developing secure IoMT applications has lately resulted in many cyber incidents directed toward such IoMT applications. The novelty of this work is to develop a framework that resolves such issues from the early stages of development. The main purpose of this framework is to provide a roadmap consisting of several strategic approaches for developing secure IoMT applications that take into consideration the advancements in artificial intelligence. The framework will also guide IoMT developers on how to mitigate and detect vulnerabilities, and hence the cyberattacks associated with each layer of a specific IoMT, using relevant machine/deep learning methods.

Keywords*: Cybersecurity; Security Attacks; Artificial Intelligence; Internet of Medical Things (IoMT); Big Data.*

1. INTRODUCTION

Smart healthcare is one concept that has received much attention lately [1]. This concept can be defined as the use of intelligent resources (such as sensors) to collect data, transmit them through the Internet of Things (IoTs), and process them using specific devices (e.g., supercomputers) [2]. Smart healthcare is a terminology that identifies systems that dynamically use intelligent methods to provide health services [1]. In other words, smart healthcare is the ecosystem that connects all parties in the medical field (patients, doctors, and hospitals) with the designated services for each of them. Such an ecosystem would provide medical services, such as assistance in diagnosing diseases and suggesting treatments [3], health management [4], prevention of disease breakout [5], and medical intelligent virtual assistants [6].

Big data is one of the most promising, emerging technologies that provide more advancements in various issues faced globally [7], and of course, healthcare is one of the most important ones. Although there are many diverse medical devices that generate a huge volume of data continuously, such diversity has resulted in issues related to the complexity and heterogeneity of such data [8]. These issues have raised a number of concerns that many patients have been questioning lately, which are mostly related to the privacy and security of patients using those technologies [9] [10].

A large volume of medical data is collected from devices using the technology of the Internet of Medical Things (IoMT). In fact, some studies expect that by 2022, there will be more than 20 billion devices connected through any form of IoT [11]. Of course, there is a major concern about the data in these devices being exploited by unauthorized users. This has resulted in many studies aiming to identify how to make the IoMT more secure with regard to securing the entire data flow process. Moreover, there are a number of vulnerabilities associated with every layer of the IoMT architecture. If such vulnerabilities are exposed by adversaries, then cyber-attacks might take place on such devices. A common vulnerability that commonly occurs within IoMT is when access controls are not properly configured, which might cause Same-Nonce attacks [12].

There is a novelty in this study, as this is the first paper that addresses the challenges associated with the management of developing secure IoMT applications. It has been lately noticed that a considerable number of attacks faced by these technologies are toward AI-enabled IoMT applications, for various reasons, rather than the traditional IoMT devices. Most efforts to avoid such attacks are directed toward defining solutions for securing IoMT technologies either from a configuration or technology perspective. Developing a framework that resolves such issues from the early stages of development is thus a must. Such framework has to be able to provide a roadmap consisting of several strategic approaches for developing secure IoMT applications, which take into consideration the advancements in artificial intelligence. This paper aims to achieve this goal by proposing a number of contributions, which are summarized as follows.

- A framework that is considered to be a roadmap for developing secure IoMT applications.
- A set of well-structured documents that can guide developers in the entire process of developing secure IoMT applications.
- A scorecard assessment methodology for monitoring and measuring the security requirements involved during IoMT development.

The remainder of this paper is structured as follows. Section 2 provides a literature review that analyses the gap in the existing secure development frameworks for IoMT applications. Section 3 illustrates the framework proposed in this paper in more detail. Section 4 shows a sample implementation of this framework and its different components. Sections 5 concludes this paper and provides suggestions for future work.

2. LITERATURE REVIEW

With the emerging technological advancements in the field of medical informatics, meeting the needs of patients in a very effective and proficient manner is a must. Intelligent telemedicine applications are gaining more popularity now as they have become powered by artificial intelligence and IoT [33]. Furthermore, IoMT can also provide many advancements in the area of healthcare and medical domains, especially when powered with artificial intelligence. An example would be the work conducted by Godi et al. [34], which suggested a monitoring system for patients in/out of hospitals using wearable devices. The system would be powered with machine learning techniques to provide monitoring, connecting, and health diagnosing services for medical staff on the health status of their patients [34].

Many of the latest emerging technologies heavily rely on big data technologies for collecting data to accomplish their objectives. In particular, technologies that are focused on big data on healthcare are considered to be crucially important in terms of security, and hence there must be several techniques and methods to protect them [35]. Several frameworks have been developed in the literature to serve this purpose; and the study of Chandra et al. [36] identifies a number of them. Furthermore, another study, conducted by Abouelmehdi et al. [37], has surveyed most of the works in the area of security for health big data. This study has identified that most of the research in this area focuses on four domains: Authentication, Encryption, Data Masking, and Access Controls [37]. Another study has also identified that many of the works in the field of big data security are related to four major categories consisting of data management, integrity and reactive security, data privacy, and infrastructure security [38]. Another work has outlined the different mechanisms with regard to the security of health big data, such as providing double-layered architecture, authenticator-based techniques, OpenSSL encryption methods, and AES encryptions [39].

In fact, IoMT technologies can have a major role in mitigating the breakout of epidemics, such as the effective use of Watson during COVID-19 pandemic [40], which is a virtual assistant tool that was used in the efforts to mitigate COVID-19. Video teleconferencing is another vital technology that has been adapted in many medical facilities in order to reduce the number of visits to hospitals [41], and it has hence provided more efficient and safe health consultations.

In many cases, the security of IoMT has been investigated with regard to the types of security attacks faced by such technologies. A recent study conducted by Papaioannou et al. [42] has surveyed several studies that identified security attacks targeting IoMT, mapping them to specific security properties. For example, it has been shown that cyberattacks, such as traffic analysis attacks, impersonation attacks, and interrogation attacks, aim to attack data confidentiality in IoMT applications [42]. Another study in this regard has surveyed the existing works that show how to adhere to the most popular security properties (i.e., confidentiality, integrity, and availability) with regard to specific models within IoMT, such as device security, cloud security, and connectivity security [43]. A further study has surveyed the technologies used in securing specific domains related to data transmission, authentication, confidentiality, access control, and privacy-preserving [44].

The most common approach that has lately gained more popularity is the use of artificial intelligent methods in detecting anomalies and cyber-attacks (e.g., machine and deep learning classifiers). The study of Hameed et al. [45] surveyed the existing works in this area that aimed to provide secure solutions in several domains. However, the most popular works were related to anomaly detection (37%), authentication and access controls (28%), intrusion detection (28%), and malware detection (7%) [45]. Another similar study was conducted by Arora et al. [46], focusing on the various types of tools used within the IoMT domain, including their security concerns, and machine learning approaches to resolve these issues. A very specific study in this field investigated the different types of malwares targeting IoMT and the machine learning techniques that would detect them [47]. Similarly, other works have been conducted to identify different techniques of intrusion detections in IoMT, and how to mitigate them using machine/deep learning algorithms [48] [49].

Table 1 shows a detailed investigation of several works that have been conducted on providing secure solutions for IoMT applications. This analysis has been done in a number of domains that are considered to be crucial for the development of secure IoMT systems. These domains consist of studies that takes into account the following issues: IoMT layers, security principles, security properties, security vulnerabilities, security attacks, AI classifiers, and security assessments. The main purpose of this analysis is to identify the gap in the existing research, which would eventually help in developing more secure IoMT solutions. Hence, the most optimal solution for developing secure IoMT technologies would be the one that considers these domains from the early stages of development, which is proposed in this paper.

Table 1: IoMT Security Development Domains Comparisons

Study	IoMT Security Development Domains						
	IoMT layers	Security Principles	Security Properties	Security Vulnerabilities	Security Attacks	AI Classifiers	Security Assessment
Alsubaei et al. [13]	√	X	X	√	√	X	√
Rizk et al. [14]	√	X	X	√	√	X	X
Rahman et al. [15]	X	X	X	√	√	X	X
Khan et al. [16]	X	X	X	√	√	√	X
Mehbodniya et al. [17]	√	X	√	√	X	X	X
Allouzi et al. [18]	X	X	X	√	X	X	√
Ahmed et al. [19]	√	X	X	√	X	√	X
Kavitha et al. [20]	X	X	X	√	X	X	X
Yu et al. [21]	X	√	√	√	X	X	X
Binbusayyis et al. [22]	X	X	X	√	√	√	X
Kumar et al. [23]	X	X	X	√	√	√	X
Wang et al. [24]	X	X	X	√	√	X	√
Kang et al. [25]	X	X	√	√	X	X	X
Almogren et al. [26]	√	X	X	√	√	X	X
Nayak et al. [27]	X	X	X	√	√	√	X
Rahmani et al. [28]	X	X	X	√	√	√	X
Wazid et al. [29]	√	X	X	X	√	√	X
Rahmadika et al. [30]	X	X	X	X	√	√	X
Jan et al. [31]	X	X	√	√	X	X	X
Hireche et al. [32]	X	X	√	√	X	X	X
Proposed Framework	√	√	√	√	√	√	√

As shown in the analysis conducted in Table 1, there is a vital need for a process that combines all important security domains when implementing any IoMT system through the use of AI technologies.

Therefore, the main purpose of this paper is to define a framework that considers all aspects of different security domains from the early stages of development in the IoMT devices.

3. PROPOSED IOMT SECURE FRAMEWORK

The main purpose of this section is to illustrate the proposed framework for developing secure IoMT architectures. This framework is a novel one, as it aims to address the security of IoMT architectures using AI techniques from the early stages of development. As shown previously, most of the actions taken in the process of securing IoMT are related to the security configurations of devices and networks. However, most of the current IoMTs are powered with AI models that allow them to collect data, process it to make interpretable information, and make decisions on such information. Such technologies have been lately the target of security cyber-attacks since they haven't received much attention with regard to their security. This raises an alert for security professionals to take a considerable amount of time to develop security procedures aiming to protect IoMT models from cybersecurity attacks. The proposed framework allows security practitioners to follow a measurable and well-structured system as a result of a security-strategic, goals-based process for developing secure IoMT. The various components of this framework are shown below in more detail.

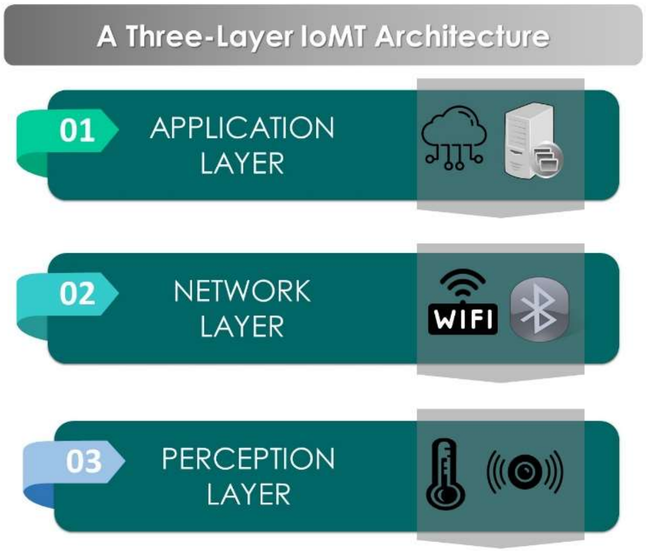


Figure 1 A Three-Layer IoMT Architecture

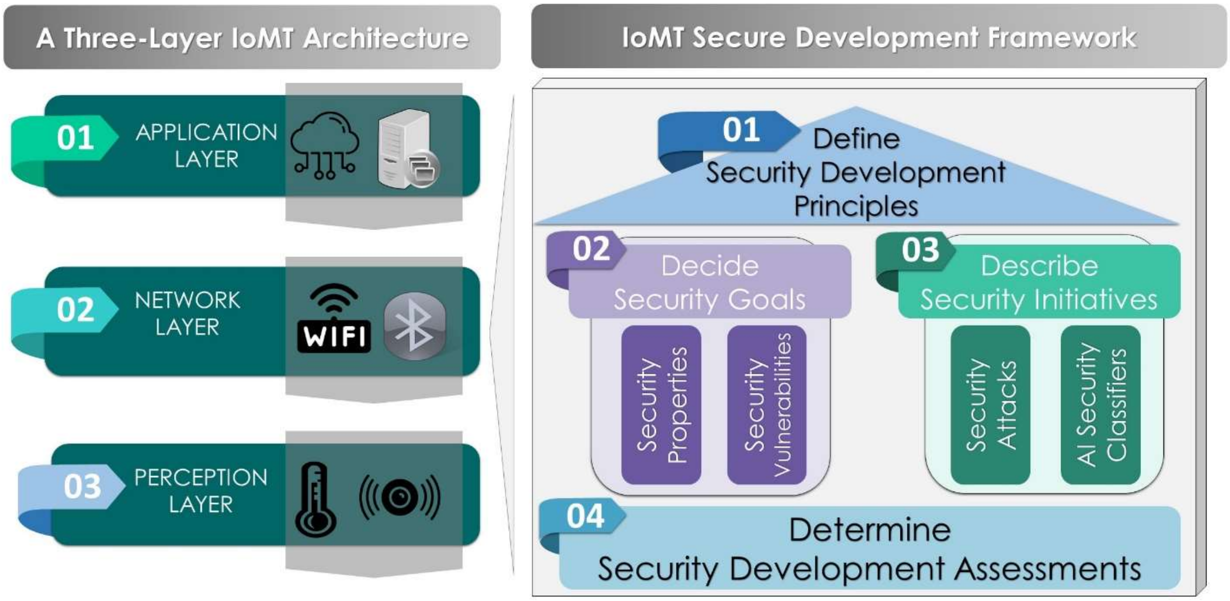

A Three-Layer IoMT Architecture
01 APPLICATION LAYER
02 NETWORK LAYER
WIFI
03 PERCEPTION LAYER
IoMT Secure Development Framework
01 Define Security Development Principles
02 Decide Security Goals
Security Properties
Security Vulnerabilities
03 Describe Security Initiatives
Security Attacks
AI Security Classifiers
04 Determine Security Development Assessments

Figure 2: Proposed IoMT Secure Development Framework

3.1. IoMT Architecture Used in Context

There are several types of IoT architectures defined in the literature, but the most common architecture for healthcare is the one consisting of three layers (perception, network, and application) [50]. As shown in Figure 1, the proposed framework in this paper is illustrated using the three-layer architecture. However, the framework proposed here is flexible enough to be applied to the other architectures (e.g., four- or five-layer architectures).

The work conducted by Srivastava et al. [51] provided a detailed explanation of the tasks implemented by the three layers in IoMT. In terms of medical devices, data sources feed the perception layer in the IoMT with data to be processed in data access sublayers. Then, this data is transformed to the network layer using methods that are considered to be short-range technologies for transmitting data, such as Bluetooth and WIFI technologies. At the network layer, several platforms are provided in order to allow any interface for network protocols to integrate with the system. The application layer is the one that provides a platform for utilizing the gathered information for managing medical information.

3.2. IoMT Secure Framework: Pillars

Figure 2 shows the different pillars of the proposed IoMT secure development framework. The proposed framework consists of four pillars, and all of them will be applicable to each layer of the considered IoMT architecture (a three-layer architecture in this work). Those four pillars represent the steps that need to be taken before developing any IoMT architecture, regardless of the type of technology being used. As explained above, this framework is designed to provide a detailed step-by-step process for developing secure IoMT architectures. The main purpose for each of the framework's four pillars (Define, Decide, Describe, and Determine) is illustrated below.

3.2.1. Pillar 01: Define Security Development Principles. This represents the first pillar in the framework, and it is responsible for defining a list of security design principles to which any IoMT application needs to adhere. Several works have investigated various security design principles, and it can be stated that the most common ones consist of reducing the attack surface size [52], applying the least privilege [53], and implementing secure defaults [54]. However, it can't be decided on specific security principles unless there is a clear understanding of the main objectives of the IoMT architecture as well as the type of environment it is operating in.

3.2.2. Pillar 02: Decide Security Goals. This pillar is related to deciding on the security goals of the IoMT architecture. Security goals are those security-oriented objectives and outcomes that an IoMT application needs to accomplish during its development process. Security goals derive their importance from the fact that they are the ones that specify how to allocate resources, prioritize efforts, align developers on certain targets, and their usability in monitoring progress. This pillar consists of two major elements that need to be developed accurately to decide on the specific strategic security goals. Once these two elements have been identified and mapped in a proper process, then it becomes much easier to choose the security goals for any IoMT application.

The first element is to select the security properties that the IoMT needs to follow to be more secure. Security properties defined for each IoMT architecture can range from one to many, depending on the number of security design principles defined in Pillar 1. The IoMT security properties, once enforced, are capable of providing secure communication between all entities within the IoMT architecture. Those properties include Confidentiality, Integrity, Availability, and Authentication, among others [55].

The other element of the second pillar is to decide on the security vulnerabilities that might occur during the deployment of IoMT applications. IoMTs could face several vulnerabilities if this crucial step is ignored until the late stages of development or, in some cases, if it is ignored entirely. Many of these vulnerabilities have been identified in several case studies. For example, not applying a proper two-factor authentication process may lead to cyber-attacks targeting data confidentiality and integrity within a specific IoMT architecture [56].

3.2.3. Pillar 03: Describe Security Initiatives. This pillar is responsible for providing a list of descriptions for security initiatives that need to be taken by IoMT security developers for the cause of developing secure IoMTs. Each initiative described consists of two major elements (i.e., security attacks faced by IoMTs and their AI detection classifiers).

Every initiative has to be related to one or many of the security goals identified in Pillar 02.

The first element here is to identify the types of cyber-attacks targeting a specific IoMT in all of its architecture layers. In fact, IoMT applications could be vulnerable to many types of cyber-attacks for various reasons. These cyber-attacks could be categorized into different domains, such as DOS and malware attacks. The most applicable approach to achieve the most outcome from this framework could be by specifying the types of attacks for each layer in the IoMT architecture. For example, it can be specified that spoofing, homing, and replay attacks may target the network layer while jamming and collision attacks may target the perception layer [57].

The second element in this pillar is to assign all cyber-attacks defined above with their detecting or mitigating AI-learning algorithms. Many machine/deep learning algorithms have been proven to be very effective in detecting several cyber-attacks targeting IoMT devices. For example, AI methods such as KNN, RF, SVM, and RNN are effective in detecting intrusion and malware attacks [58].

3.2.4. Pillar 04: Determine Security Development Assessments. One of the most successful strategies to monitor and assess progress in any particular task comes with the ability to measure (assess) its progress. One of the earliest methods used for this purpose is the use of a balanced scorecard, which was developed by Kaplan and Norton [59]. Since then, there are several works that either adopted this system to manage their strategies or modified it in a way or another to serve their objectives, and healthcare is no exception [60]. The developed scorecard for this framework is shown in Figure 3, and it consists of five elements (i.e., IoMT architecture layers, security goals, security initiatives, expected completion, actual completion, and overall progress). Therefore, it is necessary to look at this pillar to determine the activities and tasks that need to be monitored as a result of the outcomes of the previous three pillars.

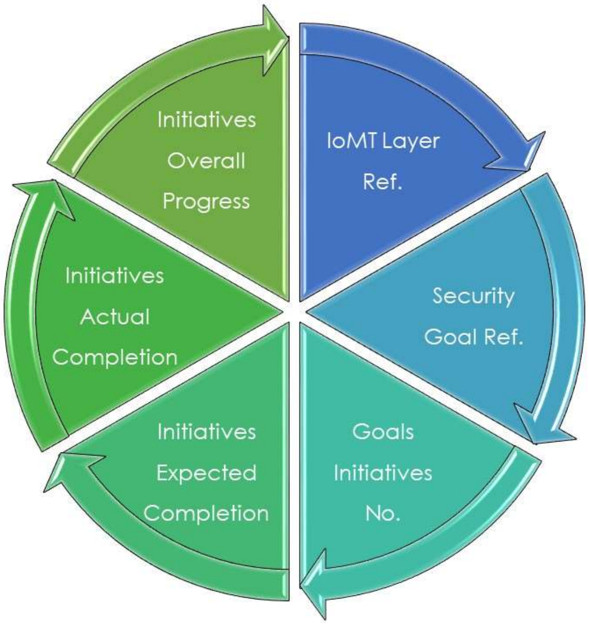

IoMT Layer Ref.
Security Goal Ref.
Goals Initiatives No.
Initiatives Expected Completion
Initiatives Actual Completion
Initiatives Overall Progress

Figure 3: Processes of IoMT Secure Development Scorecard

4. IOMT PROPOSED SECURE FRAMEWORK IMPLEMENTATION

To illustrate the implementation of the defined framework in this paper, a case study is used from the field of telemedicine, powered by IoT and AI technologies. In fact, telemedicine technologies have been used widely in the field of healthcare using several approaches and have been shown to provide very effective and efficient solutions [61]. A very useful solution of such technologies is the use of Intelligent Virtual Assistants (IVA), which were initially developed to make computer systems take actions on behalf of people using natural languages [62]. In terms of healthcare, IVAs are found to be very effective in mitigating healthcare epidemics, and recently IVAs were also used in the fight against the outbreak of the COVID-19 pandemic [63]. However, these advancements come with several challenges, particularly security challenges [64]. This section will illustrate how to implement the proposed framework in this paper in relation to Intelligent Virtual Assistants (IVA).

Intelligent Virtual Assistants (IVA) commonly interact with IoT technologies for healthcare purposes in order to provide services, such as heart rate pressure monitoring or even tracking activities of patients. Such systems would require a higher level of security compared to other systems

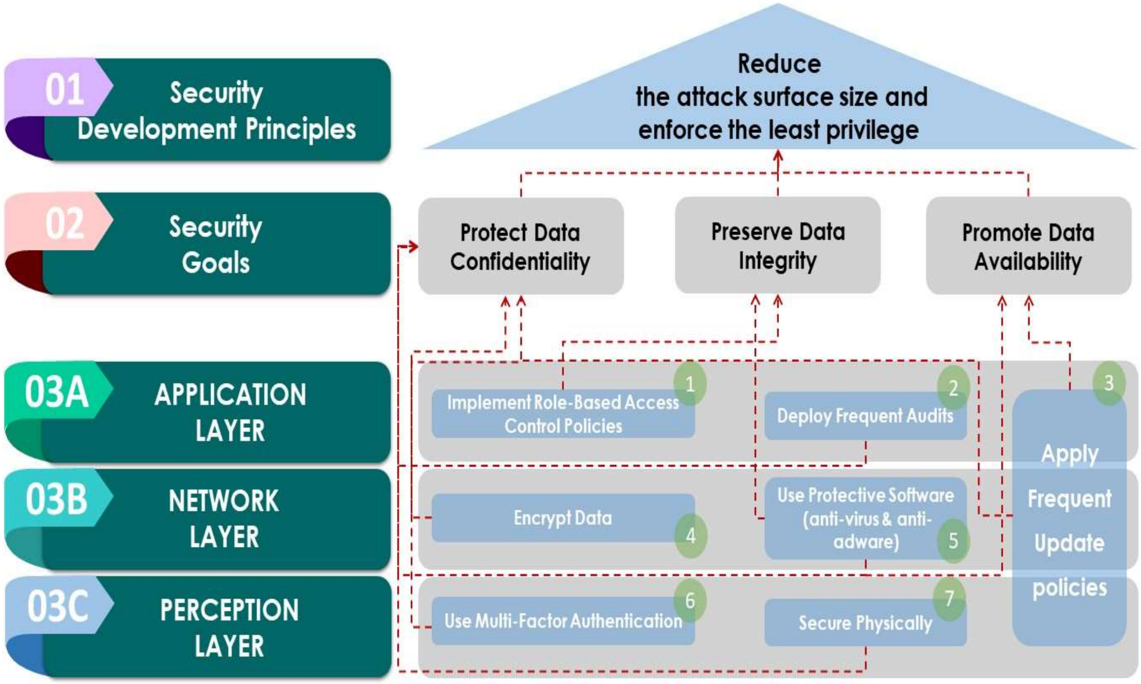

01 Security Development Principles
02 Security Goals
03A APPLICATION LAYER
03B NETWORK LAYER
03C PERCEPTION LAYER
Reduce the attack surface size and enforce the least privilege
Protect Data Confidentiality
Preserve Data Integrity
Promote Data Availability
1 Implement Role-Based Access Control Policies
2 Deploy Frequent Audits
3 Apply Frequent Update policies
4 Encrypt Data
5 Use Protective Software (anti-virus & anti-adware)
6 Use Multi-Factor Authentication
7 Secure Physically

Figure 4: IoMT Secure Development Framework Map

using IoT technologies. In fact, it requires more enforcement of security principles and policies in order to provide a high level of security.

This framework comes up with three main documents that are developed as a contribution of this work in order to make the framework more useful and achieve its objectives. These three documents consist of a framework map, a framework initiatives plan, and a framework scorecard. For the case of IVA, the various steps of the proposed framework are illustrated as follows.

4.1. Step 01: Framework Map Implementation

The first document of this framework is the framework map responsible for mapping the identified security development principles with their relevant security goals. It consists of three parts: the first is for the security development principles, the second is for identifying security properties, and the third is for the selected security goals. The objective of this document is to map these three elements with the relevant IoMT architecture layers.

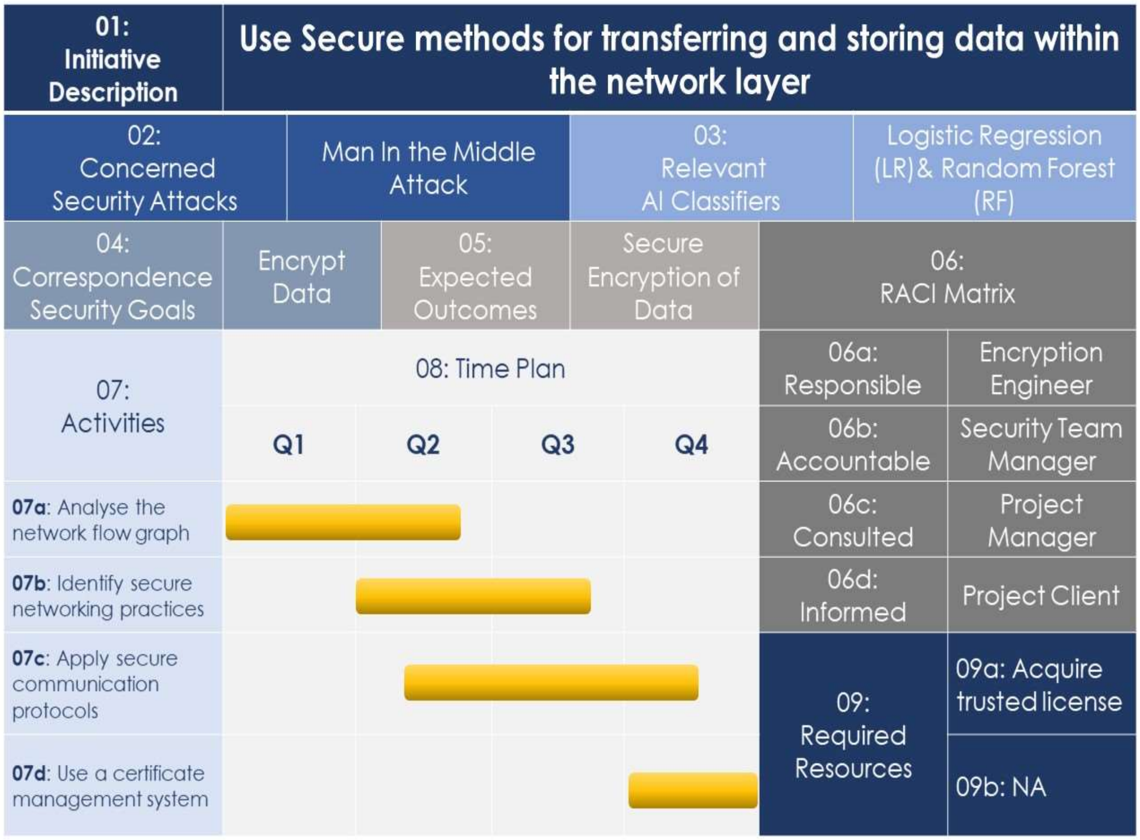
Figure 4 shows a small scale of the framework map for a specific IVA that is powered with AI models. For the chosen case study, several studies and reports have been investigated (e.g., the work of [65]) in order to select some of the most relevant security design principles, security properties, and security practices.

The first step in developing this map is to define the security development principles which are specific to the chosen case study, and this is supposed to be part of "Reduce the attack surface size and enforce the least privilege." The second step is to choose the security properties based on their applicability to the selected security principles. These security properties consist of Protect Data Confidentiality, Preserve Data Integrity, and Promote Data Availability. The third step is to define the security goals of the IoMT architecture for that particular case and map them to specific IoMT architecture layers and their correspondence security properties. There are several security goals that have been identified for the case study here, and their mapping with different security properties and IoMT layers is shown in Figure 4. The seven security goals are specified as follows:

- Implement Role-Based Access Control Policies
- Deploy Frequent Audits
- Encrypt Data
- Use Protective Software (anti-virus and anti-adware)
- Use Multi-Factor Authentication
- Secure Physically
- Apply Frequent Update policies.

4.2. Step 02: Framework Initiatives Description Implementation

The second major document for developing a secure framework for IoMT technologies is the initiatives description document. Its main aim is to clearly document each initiative for developing a secure architecture and its different processes. The major advancement of this document is that it involves combining several related parts of the existing methodologies commonly used in project management, such as the RACI matrix [66]. This document has also several items that have been the focus, such as AI-detection algorithms for specific cyber-attacks. This document consists of nine different items, which are described below.



01: Initiative Description | Use Secure methods for transferring and storing data within the network layer

02: Concerned Security Attacks | Man In the Middle Attack

03: Relevant AI Classifiers | Logistic Regression (LR) & Random Forest (RF)

04: Correspondence Security Goals | Encrypt Data

05: Expected Outcomes | Secure Encryption of Data

06: RACI Matrix

06a: Responsible	Encryption Engineer
06b: Accountable	Security Team Manager
06c: Consulted	Project Manager
06d: Informed	Project Client

07: Activities | 08: Time Plan

07: Activities	Q1	Q2	Q3	Q4
07a: Analyse the network flow graph	▬	▬		
07b: Identify secure networking practices		▬	▬	
07c: Apply secure communication protocols		▬	▬	
07d: Use a certificate management system				▬

09: Required Resources

09a: Acquire trusted license

09b: NA

Figure 5: IoMT Secure Development Framework Initiatives Description

1) Initiative Description: This item gives a clear description of the initiative and its objectives.

2) Concerned Security Attacks: This item identifies the security attacks that are relevant to that specific IoMT layer.

3) Relevant AI Classifiers: This identifies artificial intelligence learning algorithms that can be applied to detect the security attacks identified in the previous item.

4) Correspondence Security Goals: It identifies the security goals related to this initiative, extracted from the framework map.

5) Expected Outcomes: It shows the outcomes of each initiative that can be measured in the following steps by this framework.

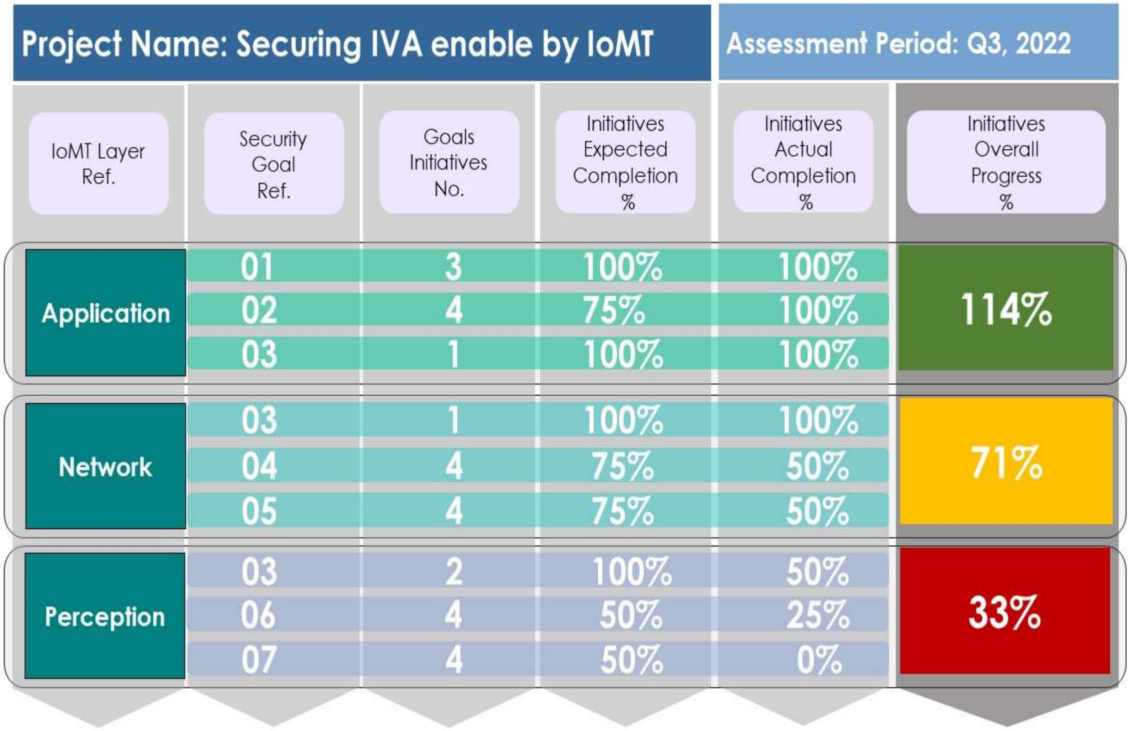
RACI Matrix: This clearly identifies teams associated with the development of each initiative from four perspectives (Responsibility, Accountability, Consulted, and Informed).

6) Activities: This is to identify the various steps/activities that need to be implemented to achieve the outcomes of each initiative.

7) Time Plan: A detailed timeline of the starting and ending period/time for each of the identified activities.

8) Required Resources: This item is the one responsible for identifying the required resources (e.g., budget, personnel, or others) to have a successful implementation of each initiative.

To elaborate more on this part, a sample of a specific initiative for the IVA case study has been constructed based on the information collected from several works, such as [67] and [68]. This initiative description document has been shown in more detail in Figure 5. The first item in this document shows the initiative's name, which has been identified as "Use secure methods for transferring and storing data within the network layer." This initiative aims to mitigate the security attacks of Man in the Middle using several machine learning algorithms (e.g., LR and RF) as described in items 02 and 03 respectively. The initiative is associated with the security goal of Encrypt Data at the network layer, as shown in item 04. Item 05 is the one responsible for identifying the final outcomes of this initiative, which is to ensure secure encryptions of data. The distribution of responsibilities for implementing this initiative is outlined in item 06 using the RACI matrix. The different activities that need to be taken along with their timelines are shown in items 07 and 08 respectively. Item 09 is the one which shows the required resources in order for this initiative to be implemented successfully, which is to purchase specific licenses for that specific initiative.



Project Name: Securing IVA enable by IoMT

Assessment Period: Q3, 2022

IoMT Layer Ref.	Security Goal Ref.	Goals Initiatives No.	Initiatives Expected Completion %	Initiatives Actual Completion %	Initiatives Overall Progress %
Application	01	3	100%	100%	114%
	02	4	75%	100%	
	03	1	100%	100%	
Network	03	1	100%	100%	71%
	04	4	75%	50%	
	05	4	75%	50%	
Perception	03	2	100%	50%	33%
	06	4	50%	25%	
	07	4	50%	0%	

Figure 6: IoMT Secure Development Framework Scorecard

4.3. Step 03: Framework Scorecard Implementation

This represents the third document of the proposed framework in this paper which is to introduce a scorecard assessment process. The main goal of this scorecard is to measure the progress of all initiatives in any case, considering specific security goals in reference to a specific IoMT architecture layer. This scorecard can be described as an initiative-based assessment system, and hence, this would allow to monitor the progress of developing secure IoMT technologies and enhance quality assurance more efficiently. Figure 6 shows a sample of this document, and it consists of several items, which are outlined as follows.

1) IoMT Layer Ref.: This represents the specific layer against which the progress of security goals and initiatives need to be measured.

2) Security Goal Ref.: This item shows the reference of every security goal as defined in the framework map, against which their progresses need to be assessed and monitored.

3) Goals Initiatives No.: This item shows the number of initiatives for a particular IoMT layer and security goals that need to be assessed.

4) Initiatives Expected Completion: This item identifies the expected completion percentage for all initiatives associated with every security goal in a specific IoMT layer.

5) Initiatives Actual Completion: This item identifies the actual completion percentage for all initiatives associated with every security goal in a specific IoMT layer.

6) Initiatives' Overall Progress: This item is the last one in the scorecard document and is responsible for showing the overall progress for all initiatives and security goals in a particular IoMT layer. It can represent the progress in three different categories (Green: indicating on progress; Amber: indicating slightly below progress; and Red: indicating heavily behind progress).

From the sample scorecard assessment in Figure 6, it can be seen that the application layer has three security goals, as documented in the framework map. Security goal (1), for instance, has three initiatives, their expected completion percentage at that period of time is 100%, and their actual completion percentage is 100%. The initiatives' overall progress for the application layer shows that it is 114%, and this indicates that there are initiatives that have been completed ahead of their scheduled time. Another example is shown in security goal (7) of the perception layer, with four initiatives, and their expected completion percentage at the period of assessment is supposed to be 50%. However, the actual completion percentage of those four initiatives is 0%, which means that none of them has been initiated. The low performance of completing these four initiatives along with the other six ones for the perception layer have resulted in a low percentage of the overall completion for that particular IoMT layer (i.e., the perception layer).

5. CONCLUSION AND FUTURE WORK

The latest expansions in the use of IoMT technologies have made such technologies experience new risks. Many of these risks are associated with the complexity and het- erogeneity of IoMT architectures and are directed toward exposing their security, which if done can lead to severe outcomes. The security of IoMT applications has been investigated in several works, but there is a great need for defining an efficient and effective security framework that manages all processes of developing secure IoMT applications. Many of the currently used plans are related to the general practices of developing secure systems while IoMTs require special considerations and planning in this regard. Therefore, this work proposes a novel framework that aims to resolve most weaknesses of the several security frameworks in the development of IoMT applications.

The novelty of this framework lies in it taking into account the security difficulties and challenges associated with IoMTs from the early stages of development. This framework considers the different characteristics and steps of security practices associated with IoMTs. It ensures that security design principles and security properties are considered, followed, and measured throughout the entire process of development. It also aims to specify security practices in an initiative-based approach that need to be well documented from the start of development. This would enable accurate assessment of completion and adherence at any period during development. The framework also allows developers to identify cybersecurity attacks associated with each layer of the IoMT architecture, and their AI-mitigating methods. This would make the detection and mitigating steps of cyberattacks to be considered and tested from the early stages, even before the actual deployment. The framework thus defines three major documents related to mapping the security goals with secure initiatives, defining detailed activities for each initiative in a timeline approach, and assessing the progress of adherence to security goals at any time.

Future extensions to this work could be presented in several areas. The most important one is related to the development of a tool that automates all the different processes of this framework. In fact, when this framework is automated, then the assessment process could provide more accessibility and easy monitoring at any stage. However, the most crucial and challenging extension of this work is the integration of the proposed framework with other existing frameworks used for purposes other than security for the development of IoMT technologies. Without any doubt, such developments could lead to more reliable technologies this regard.

REFERENCES

[1] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," *Global Health Journal*, vol. 3, no. 3, pp. 62–65, 2019.

[2] J. L. Martin, H. Varilly, J. Cohn, and G. R. Wightwick, "Preface: Technologies for a smarter planet," *IBM Journal of Research and Development*, vol. 54, no. 4, pp. 1–2, 2010.

[3] J. Dhar and A. Ranganathan, "Machine learning capabilities in medi- cal diagnosis applications: computational results for hepatitis disease," *International Journal of Biomedical Engineering and Technology*, vol. 17, no. 4, pp. 330–340, 2015.

[4] J. Andreu-Perez, D. R. Leff, H. M. D. Ip, and G.-Z. Yang, "From wearable sensors to smart implants—toward pervasive and person- alized healthcare," *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 12, pp. 2750–2762, 2015.

[5] J. Redfern, "Smart health and innovation: facilitating health-related behaviour change," *Proceedings of the Nutrition Society*, vol. 76, no. 3, p. 328–332, 2017.

[6] P.-J. Yang and W.-T. Fu, "Mindbot: a social-based medical virtual assistant," in *2016 IEEE International Conference on Healthcare Informatics (ICHI)*, pp. 319–319, IEEE, 2016.

[7] J. Wu, S. Guo, J. Li, and D. Zeng, "Big Data Meet Green Challenges: Big Data Toward Green Applications," *IEEE Systems Journal*, vol. 10, no. 3, pp. 888–900, 2016.

[8] I. D. Dinov, "Methodological challenges and analytic opportunities for modeling and interpreting Big Healthcare Data," *GigaScience*, vol. 5, no. 02 2016. s13742-016-0117-6.

[9] W. N. Price and I. G. Cohen, "Privacy in the age of medical big data," *Nature medicine*, vol. 25, no. 1, pp. 37–43, 2019.

[10] M. Mallappallil, J. Sabu, A. Gruessner, and M. Salifu, "A review of big data and medical research," *SAGE Open Medicine*, vol. 8, p. 2050312120934839, 2020. PMID: 32637104.

[11] R. Kandaswamy, D. Furlonger, *et al.*, "Blockchain-based transforma- tion," *https://www. gartner. com/en/doc/3869696-blockchain-based- transformation-a-gartner-trend-insight-report*, 2021.

[12] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Gly- nos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors*, vol. 20, no. 17, 2020.

[13] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "Iomt-saf: Internet of medical things security assessment framework," *Internet of Things*, vol. 8, p. 100123, 2019.

[14] D. Rizk, R. Rizk, and S. Hsu, "Applied layered-security model to iomt," in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 227–227, 2019.

[15] M. Rahman and H. Jahankhani, *Security Vulnerabilities in Existing Security Mechanisms for IoMT and Potential Solutions for Mitigating Cyber-Attacks*, pp. 307–334. Cham: Springer International Publish- ing, 2021.

[16] I. A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, and B. S. Ali, "Xsru-iomt: Explainable simple recurrent units for threat detection in internet of medical things networks," *Future Generation Computer Systems*, vol. 127, pp. 181–193, 2022.

[17] A. Mehbodniya, R. Neware, S. Vyas, M. R. Kumar, P. Ngulube, and S. Ray, "Blockchain and ipfs integrated framework in bilevel fog- cloud network for security and privacy of iomt devices," *Computa- tional and Mathematical Methods in Medicine*, vol. 2021, 2021.

[18] M. A. Allouzi and J. I. Khan, "Identifying and modeling security threats for iomt edge network using markov chain and common vulnerability scoring system (cvss)," 2021.

[19] J. Ahmed, T. N. Nguyen, B. Ali, A. Javed, and J. Mirza, "On the physical layer security of federated learning based iomt networks," *IEEE Journal of Biomedical and Health Informatics*,

pp. 1–1, 2022.

[20] D. Kavitha and C. Subramaniam, "Security threat management by software obfuscation for privacy in internet of medical thing (iomt) application," *Journal of Computational and Theoretical Nanoscience*, vol. 14, no. 7, pp. 3100–3114, 2017.

[21] S. Yu and K. Park, "Sals-tmis: Secure, anonymous, and lightweight privacy-preserving scheme for iomt-enabled tmis environments," *IEEE Access*, vol. 10, pp. 60534–60549, 2022.

[22] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, "An inves- tigation and comparison of machine learning approaches for intrusion detection in iomt network," *J. Supercomput.*, vol. 78, p. 17403–17422, oct 2022.

[23] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," *Computer Communications*, vol. 166, pp. 110–124, 2021.

[24] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "Isa evaluation framework for security of internet of health things system using ahp-topsis methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.

[25] J. Kang, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "An ultra light weight and secure rfid batch authentication scheme for iomt," *Computer Communications*, vol. 167, pp. 48–54, 2021.

[26] A. Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "Ftm-iomt: Fuzzy-based trust management for preventing sybil at- tacks in internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4485–4497, 2021.

[27] J. Nayak, S. K. Meher, A. Souri, B. Naik, and S. Vimal, "Ex- treme learning machine and bayesian optimization-driven intelligent framework for iomt cyber-attack detection," *J. Supercomput.*, vol. 78, p. 14866–14891, 2022.

[28] M. K. I. Rahmani, M. Shuaib, S. Alam, S. T. Siddiqui, S. Ah- mad, S. Bhatia, and A. Mashat, "Blockchain-based trust management framework for cloud computing-based internet of medical things (iomt): A systematic review," *Computational Intelligence and Neuro- science*, vol. 2022, 2022.

[29] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. P. C. Rodrigues, "Ascp-iomt: Ai-enabled lightweight secure communica- tion protocol for internet of medical things," *IEEE Access*, vol. 10, pp. 57990–58004, 2022.

[30] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for mis- behavior detection in lightweight iomt devices," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–13, 2022.

[31] M. A. Jan, M. Usman, X. He, and A. Ur Rehman, "Sams: A seamless and authorized multimedia streaming framework for wmsn-based iomt," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1576–1583, 2019.

[32] R. Hireche, H. Mansouri, and A.-S. K. Pathan, *Fault Tolerance and Security Management in IoMT*, pp. 65–104. Cham: Springer International Publishing, 2022.

[33] Intel, "Telemedicine technology powered by ai and iot," 2022. Ac- cessed Nov 1, 2022.

[34] B. Godi, S. Viswanadham, A. S. Muttipati, O. P. Samantray, and S. R. Gadiraju, "E-healthcare monitoring system using iot with machine learning approaches," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp. 1–5, 2020.

[35] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in *2014 IEEE International Congress on Big Data (BigData Congress)*, (Los Alamitos, CA, USA), pp. 762–765, IEEE Computer Society, 2014.

[36]

[37] S. Chandra, S. Ray, and R. Goswami, "Big data security in healthcare: Survey on frameworks and algorithms," in *2017 IEEE 7th International Advance Computing Conference (IACC)*, (Los Alamitos, CA, USA), pp. 89–94, IEEE Computer Society, jan 2017.

[38] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Com- puter Science*, vol. 113, pp. 73–80, 2017. The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2017) / Affiliated Workshops.

[39] A. Khanan, S. Abdullah, A. H. H. M. Mohamed, A. Mehmood, and K. A. Z. Ariffin, "Big data security and privacy concerns: A

review," in *Smart Technologies and Innovation for a Sustainable Fu- ture* (A. Al-Masri and K. Curran, eds.), (Cham), pp. 55–61, Springer International Publishing, 2019.

[40] S. Hamrioui, I. de la Torre D´ıez, B. Garcia-Zapirain, K. Saleem, and J. J. Rodrigues, "A systematic review of security mechanisms for big data in health and new alternatives for hospitals," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[41] IBM, "IBM Watson," Sept. 2020. https://www.ibm.com/watson/covid-response.

[42] J. E. Hollander and B. G. Carr, "Virtually perfect? telemedicine for covid-19," *New England Journal of Medicine*, vol. 382, no. 18, pp. 1679–1681, 2020.

[43] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (iomt)," *Transac- tions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e4049, 2022.

[44] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 457–464, 2019.

[45] T. Vaiyapuri, A. Binbusayyis, and V. Varadarajan, "Security, privacy and trust in iomt enabled smart healthcare system: a systematic review of current and future trends," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 2, 2021.

[46] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches," *PeerJ Computer Science*, vol. 7, p. e414, 2021.

[47] P. Arora, B. Kaur, and M. A. Teixeira, "Machine learning-based secu- rity solutions for healthcare: An overview," in *Emerging Technologies for Computing, Communication and Smart Cities* (P. K. Singh, M. H. Kolekar, S. Tanwar, S. T. Wierzchon´, and R. K. Bhatnagar, eds.), (Singapore), pp. 649–659, Springer Nature Singapore, 2022.

[48] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "Iomt malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[49] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, "Machine learning and deep learning methods for intrusion detection systems in iomt: A survey," in *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, pp. 1–9, 2022.

[50] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured iomt framework based on swarm-neural network," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1969–1976, 2022.

[51] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, 2018.

[52] J. Srivastava, S. Routray, S. Ahmad, and M. M. Waris, "Internet of medical things (iomt)-based smart healthcare system: Trends and progress," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[53] ENISA, "GOOD PRACTICESFOR SECURITY OFIOT," techreport, European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/good-practices-for-security- of-iot-1, Nov. 2019.

[54] UL Solutions, "IoT SecurityTop 20 Design Principles," resre- port, UL Solutions, https://www.ul.com/resources/iot-security-top-20- design-principles, 2019.

[55] A. Raja, "IoT Security by Design," Mar. 2019. https://www.iotforall.com/iot-security-by-design.

[56] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective mea- sures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341, 2015.

[57] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2021.

[58] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, “Se- curity vulnerabilities and intelligent solutions for iomt systems,” in *Internet of Medical Things*, pp. 175–194, Springer, 2021.

[59] D. Unal, S. Bennbaia, and F. O. Catak, “Chapter 12 - machine learning for the security of healthcare systems based on internet of things and edge computing**qatar national research fund,” in *Cybersecurity and Cognitive Science* (A. A. Moustafa, ed.), pp. 299– 320, Academic Press, 2022.

[60] R. S. Kaplan and D. P. Norton, *Balanced Scorecard*, pp. 137–148. Wiesbaden: Gabler, 2007.

[61] W. N. Zelman, G. H. Pink, and C. B. Matthias, “Use of the balanced scorecard in health care,” *Journal of health care finance*, vol. 29, no. 4, p. 1—16, 2003.

[62] N. Lurie and B. G. Carr, “The Role of Telehealth in the Medical Response to Disasters,” *JAMA Internal Medicine*, vol. 178, pp. 745– 746, 2018.

[63] J. Biljon and P. Kotze´, “Modelling the factors that influence mobile phone adoption,” vol. 226, pp. 152–161, 01 2007.

[64] M. F. Nihla, W. W. Arachchi, K. D. Subhani, D. Dissanayaka,
W. Sanduni, W. Rankothge, P. Wariyapperuma, and P. Kehelella, “Andti virtual assistant,” in *2022 2nd International Conference on Image Processing and Robotics (ICIPRob)*, pp. 1–6, 2022.

[65] S. Callens, “Telemedicine and european law,” *Medicine and law*, vol. 22, pp. 733–41, 02 2003.

[66] OWASP, “Owasp internet of things project,” 2018.
https://wiki.owasp.org/index.php/OWASP Internet of Things Project #tab=IoT Top 10.

[67] P. Khan and K. A. Quraishi, “Impact of raci on delivery and outcome of software development projects,” in *2014 Fourth International Conference on Advanced Computing & Communication Technologies*,
pp. 177–184, 2014.

[68] R. Mohanakrishnan, “What is a man-in-the-middle attack? definition, detection, and prevention best practices for 2022,” Apr. 2022. https://www.spiceworks.com/it-security/data-security/articles/man-in- the-middle-attack/.

[69] O. Toutsop, P. Harvey, and K. Kornegay, “Monitoring and detection time optimization of man in the middle attacks using machine learn- ing,” in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, pp. 1–7, 2020.