IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 October 2022, accepted 23 November 2022, date of publication 28 November 2022,
date of current version 2 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3225038

SURVEY

A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)

TAQWA AHMED ALHAJ[1,5], SETTANA MOHAMMED ABDULLA[2], MOHMMED ABDULLA ELSHEKH IDERSS[3], ALAA ABDALATI AHMED ALI[2], FATIN A. ELHAJ[4,5], MUHAMMAD AKMAL REMLI[1,6], AND LUBNA ABDELKAREIM GABRALLA[7]

[1]Institute for Artificial Intelligence and Big Data, Universiti Malaysia Kelantan, City Campus, Pengkalan Chepa, Kota Bharu, Kelantan 16100, Malaysia
[2]Solutize Integrated Solution, Khartoum 11115, Sudan
[3]Thiqah Business Services, Riyadh 13321, Saudi Arabia
[4]College of Arts, Science and Information Technology, University of Khorfakkan, Khor Fakkan, United Arab Emirates
[5]Faulty of Mathematical Sciences and Informatics, University of Khartoum, Khartoum 11111, Sudan
[6]Faculty of Data Science and Computing, Universiti Malaysia Kelantan, City Campus, Pengkalan Chepa, Kota Bharu, Kelantan 16100, Malaysia
[7]Department of Computer Science and Information Technology, College of Applied, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding author: Taqwa Ahmed Alhaj (taqwa-315@hotmail.com)

This work was supported by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through the Princess Nourah bint Abdulrahman University Researchers Supporting Project under Grant PNURSP2022R178.

ABSTRACT The integration of medical equipment into the Internet of Things (IoT) led to the introduction of Internet of Medical Things (IoMT). Variation of IoT devices have been equipped in medical facilities. These devices provided convenience to healthcare provider since they can continuously monitor their patients in real-time, while allowing them to have greater physical flexibility and mobility. However, users of healthcare services (such as patients and medical staff) often are less concerned about security issues associated with IoT. These alleviate existing problems and jeopardize the lives of their patients by making them susceptible to attacks. Furthermore, IoMT applications have direct access to healthcare services because it handles sensitive patient information. Therefore, it is extremely important to preserve and establish the security and privacy of IoMT. This further justifies the need to investigate and address the related issues. Despite existing literature on security and privacy mechanisms, the domain still requires more attention. Therefore, this paper aims to discuss the security and privacy principles, as well as challenges associated with IoMT. Besides, a comprehensive analysis of privacy and security solutions for IoMT is also presented. In addition, we introduced a novel taxonomy of IoMT security and privacy based on cyber security principles such as ''govern,'' ''protect,'' and ''detect''. In conclusion, this paper provides a discussion on existing challenges and future direction for researchers.

INDEX TERMS IoT, IoMT, security, privacy, govern, protect, detect.

I. INTRODUCTION

Healthcare systems need to handle variations of illnesses and treatments with an increased number of patients. The use of telemedicine systems are useful since patient can be treated at home, hence reducing the overtaxed costs of healthcare infrastructures [1]. Therefore, the development of Internet of Things (IoT) is expected to substantially improve the efficiency and standard treatment in the healthcare industry which further known as the Internet of Healthcare (IoHT) or the Internet of Medical Things (IoMT) [2]. Specifically, IoMT can assist with the requirement of more genericity and scalability [1]. Many healthcare practitioners use IoMT applications to improve therapy, disease control, failure reduction, drug prescription management, and cost savings [3]. Furthermore, IoMT tremendously advances healthcare systems by expediting procedures that enable the adoption of cutting-edge diagnostic and therapeutic techniques via connected wearable sensor devices and real-time monitoring data available from IoT technologies [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

However, the dynamic architecture and openness of IoMT has led to an increased vulnerabilities in terms of security and privacy. Particularly, many security issues arise because of IoMT application usage including unauthorized access to user data, unauthorized remote control of smart devices, wasteful third-party use of personnel data, and so on [5].

Therefore, it is critical to address these security and privacy concerns, as well as associated attacks and drawbacks with a security maintenance. The basic structure of ontology includes elements such as concepts, relations, examples, and axioms. In the IoMT model, concepts represent a collection of entities. Whereas relations describe how concepts interact with each other. Meanwhile, axioms are defined as statements that limit the values that can be assigned to concepts or instances. This paper presents a comprehensive survey of existing literature that address these issues through the application of variety security and privacy principles. Throughout the survey, we included our points of view as a discussion. The cyber security principles, for example, are designed to provide strategic guidance on how to protect and detect IoMT systems and data from cyber threats. These cyber security concepts are classified into three groups: govern, protect, and detect. The Govern principle promotes company-wide awareness of cybersecurity risks to systems, people, assets, data, and capabilities. The Protect principle measures the precautions to secure the delivery of critical infrastructure services. Meanwhile, the Detect principle describes the procedures that must be followed to detect the onset of a cyber incident. These components are further elaborated in the following sections. The contributions of our work are highlighted as follows:

- We proposed a novel taxonomy based on cybersecurity principles such as govern, protect, and detect for IoMT security and privacy approaches.
- We provided a comprehensive classification of security principles based on different groups of their IoMT application.
- We highlighted on an open research challenges for IoMT security and privacy, and recommended potential future research area.

This survey paper introduces several key principles of the IoMT and presents the scope of our discussion in Section II. Next, Section III, investigates the existing literature on the source of information used in the security of IoMT. Following that, Section IV highlights the IoMT challenges and issues. Then, Section V discusses a comparison analysis of related surveys. Section VI provides the proposed taxonomy of IoMT security principles. Section IX summarizes the discussion and future research directions. The final section discusses the summary of the work.

II. CONCEPTS AND SCOPE

IoT is a modern paradigm shift in the realm of information technology. In general, IoT enables a more direct integration of the real world with computer-based systems, as well as increased efficiency, accuracy, and financial benefits [5]. The well-proven IoT strategy is progressing into the healthcare and medical industries, which is referred to as IoMT. IoMT refers to as the networking of communication-enabled medical equipment and their integration into broader health networks that is beneficial for the patients [1].

The architecture of IoMT is comprised of three layers, which are data gathering, data management, and medical services layer, as represented in Figure 1. The IoMT architecture has been adopted in several IoMT systems including [6]and [2].

- Data Collection Layer: this layer consists of sensors and medical equipment that collect patient data into a local network known as a Body Sensor Network (BSN) [7].
- Data Management Layer: this layer is responsible for locally processing and storing patient data generated by medical devices before it is transferred to a centralized medical server.
- Medical Service Layer: this layer allows medical personnel such as doctors to have remote access to their patients' data and provide timely advice to them. Moreover, the algorithms and computer programs for early diagnosis and assessments on the state condition of the patient is provided in this layer.

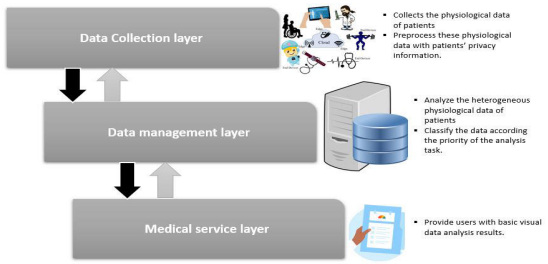


FIGURE 1. IoMT Healthcare System Architecture.

III. SOURCE OF INFORMATION

There are numerous sources of information that can substantially aid in the examination of IoMT security and privacy. In this regard, some researchers have advocated the utilization of a wide range of information sources to establish a secure IoMT system. This section examines the most relevant data sources for the IoMT systems that have been proposed.

A. ONTOLOGY DATABASE

Ontologies are powerful database repository that can be applied to a broad range of knowledge. They are composed of machine-readable definitions and formal descriptions of many concepts and relationships that exists among entities within a domain [8]. The illustration of our area of research can be presented by Alsubaei and others [9] in which they demonstrated a tool that uses a semantically enhanced ontology to represent the elements of the IoMT, security issues and solutions. The context-aware rules in the developed ontology enable reasoning to provide a recommendation system that enables users to reach well-informed decisions. The basic structure of ontology includes elements such as concepts,

relations, examples, and axioms. In the IoMT model, concepts represent a collection of entities. Whereas relations describe how concepts interact with each other. Meanwhile, axioms are defined as statements that limit the values that can be assigned to concepts or instances.

B. VULNERABILITIES DATABASE

The Vulnerabilities database mostly been studied for use in intrusion detection systems [8]. It monitors all known exploits and system vulnerabilities, as well as the security patches associated with them. It is developed by gathering information about the monitored resource configurations, such as operating systems or network application services that could be exploited by the attackers.

In [9], the authors assembled a list of documented IoMT-related issues from CVE Details and National Vulnerability Database (NVD) of NIST over the previous four years. The authors discovered 40 separate vulnerabilities after filtering all discovered vulnerabilities to eliminate those that were non-medical endpoint, for instance, those that are not relevant to IoMT. Then, they classified these flaws into 11 different scenarios. Next, they evaluated whether the tool had discovered the known vulnerability security issue for each associated scenario. The program was successful in identifying all security flaws such as absent or insufficient security measures.

In [10], the authors propose a path search algorithm that incorporates threat intelligence, solutions, stakeholders, and infrastructure. The stakeholders include medical practitioners, system or network administrators, and patients. The examples of solution include devices, services, and infrastructure. The search sought to investigate the threat intelligence issues and solutions for IoMT vulnerabilities.

The authors [11], proposed a risk study of ITS based on the threat, risk, and vulnerability analysis (TVRA) method, with an emphasis on ETSI ITS communication architecture. The TVRA methodology is based on the probability of a particular attack as well as the impact of the attack towards the system, which includes system assets and threats. Furthermore, the TVRA method identifies the threat agent attempting to compromise the system. Therefore, TVRA outputs include risk measures for previously identified threats, which can be calculated based on the probability of systemic effects.

C. INTRUSION DATABASE

Intrusion Database consists of activities that can be classified as either malicious or normal. The intrusion detection system (IDS) monitor and analyze the network traffic. The IDS system will trigger an alert if it detects any occurrences of malicious activity. Moreover, the network management agents can also trigger an alert using management protocols like SNMP traps, CMIP event reports, GrIDS, or even SCADA monitoring systems [8]. Nandy et al. [12] employed a secure IoMT framework based on Swarm-Neural Network using intrusion detection mechanism. The authors used real data known as ToN-IoT dataset for the proposed model. In [13], a deep neural network (DNN) was employed to develop an effective and efficient IDS to identify and predict unexpected cyber threats.

IV. IoMT CHALLENGES AND CONCERNS

In this section, the main concerns pertinent to IoT systems is presented with an emphasize on associated medical challenges as the following:

A. ABSENCE OF INTEROPERABILITY

There are numerous distinct sensors used for medical application with varying degrees of computer power, memory, power production, and embedded systems in the data gathering layer of the IoMT. The data formats used to collect patient physiological data vary by device, making data handling difficult in the data management layer [14]. Besides, the heterogeneity of wireless/wired protocols are another factor that contributes to poor interoperability. In such case, the medical devices collect the physiological data of patients and transfer the data to the servers. During the transmission process, various wireless protocols are used including WiFi, NB-IoT, and Bluetooth Low Energy (BLE). These are known to be used in certain powerful wearable medical sensor systems. Medical information interchange can be difficult at different medical facilities due to incompatibility between different IoMT systems [14].

B. PRIVACY AND SECURITY

The escalation of security and privacy issues are due to the dynamic architecture and openness of IoMT. According to the literature, installing IoMT applications introduced a diverse range of security issues, including unauthorized access to patient data and remote control of medical devices [5]. Patients may encounter major implications if their sensitive physiological information is disclosed [14]. Therefore, at the data management layer and health service layer, several access control mechanisms and identity authentication systems are introduced to ensure the confidentiality of sensitive patient information. [5]. However, these confidential data are still entrusted to a third party for privacy preservation, so the data server may be vulnerable to information breach. As a result, data storage may inadvertently or intentionally expose patient information [5].

C. BIG DATA ANALYTICS

According to [15], it is beneficial to evaluate healthcare through efficient illness management even though it may be time consuming. The literature introduces the CARE system, which employs big data analytics as a proactive in IoMT to support physicians in analyzing the status of their patients by enabling patient-physician interactions and sending physicians an alert when the patient's life is at risk. Another strategy for managing the massive amount of medical data is to develop an IoT-based information system for emergency medical services that unifies data formats and simplifies

data accessibility, as well as a semantic model for data storage [16].

D. ENERGY CONSUMPTION

In general, IoMT relies heavily on sensors to collect real-time data from smart devices [5]. One way to improve the efficiency of sensors' capabilities is to regulate their energy consumption to extend their life span, which prevents communication breakdowns [5]. The authors in [17] introduced several strategies to preserve sensor energy by developing powerful batteries, introducing energy efficient protocols, and establishing energy preservation access points and gateways. Many studies have focused on preserving sensor energy, such as [18], which presented a wireless sensor network based on ZigBee and WiMax radios to achieve energy efficiency by selecting the gateway with the lowest link cost based on the distance from the internet and the remaining energy of sensors. In contrary, the authors in [19] believed that the integration of cloud and IoMT would result in more efficient energy usage and management.

E. NETWORK AND PROTOCOL DESIGN CHALLENGES

A routing protocol defines the flow of data between network routers, allowing them to choose routes between any two nodes in the same or different networks. A protocol is a set of rules that govern how data is exchanged between devices. Wireless network routing algorithms are more advanced than wired network routing algorithms in several areas, including network topology, power conservation, and channel efficacy. Routing systems in wireless networks must provide more than just data transfer between nodes [2].

V. RELATED SURVEYS

Several papers have discussed the security and privacy of the IoMT, either exclusively as in [20] and [21] or indirectly as in [22], [23], [24], [22], and [21].

Gatouillat et al. [1] reviewed recent contributions that attempt to improve the IoMT by incorporating formal approaches developed by the community of Cyber-Physical Systems (CPS). They demonstrated that the CPS strategy increases system robustness, security, and dependability, as well as verification and validation. Furthermore, a comprehensive list of CPS approaches used in the IoMT was provided and discussed. They then discussed how patients and medical professionals may benefit from medical technology's accessibility. However, their research does not provide a thorough analysis of the state-of-the-art in IoMT security and privacy. Conversely, their discussion on the survey papers focus mainly on device security.

Maria Papaioannou et al. [25] categorised actual and potential risks to the IoMT edge network based on critical security targets such as: Confidentiality, integrity, non-repudiation, authentication, authorization, and availability. They also provided a classification of security countermeasures against threats to IoMT networks based on literature. However, their investigation is narrow and limited to only selected survey papers considered.

In Sun et al. [2], reviewed the security and privacy issues that IoMT systems faced. They also explored on the privacy and security needs for IoMT based on data level, sensor level, personal server level, and medical server level. As conclusion, the authors presented a general overview of the current state-of-the-art techniques. Similar to prior work, their review is not comprehensive and lacks insights on each IoMT security principles.

Yaacoub et al. [20] provided an overview and analysis of security and privacy concerns associated to medical IoT systems. In addition, the source of attacks, and attributes, as well as their extent and impacts were described and explored in detail. The study also examines contemporary lightweight security solutions that use both cryptographic and non-cryptographic methods. However, they focused more on the IoMT challenges, risks, and cyber-attacks on IoMT scenarios on related survey papers. Accordingly, their paper provides a quick rundown of the current state of IoMT security solutions.

Hatzivasilis et al. [26] provides an overview of the key security and privacy controls that must be implemented in modern IoMT settings to protect the data of users and stakeholders. Nonetheless, their study was limited to security devices, with little discussion of the state of the art for each studied technique. Therefore, our paper thoroughly examined each study from a variety of perspectives, including risk management, how to secure an IoMT system, and how to detect any suspicious activity or security incidents. It also investigated the specific requirements and challenges of IoMT systems using diverse data sources. Table1 compares existing IoMT security surveys to our findings in key areas.

VI. TAXONOMY OF IoMT SECURITY PRINCIPLES

Based on our observation on existing literature review, several efforts have been made to provide taxonomies on related IoMT security and privacy approaches. However, most of them have adopted a classification criterion based solely on a few security principles. Therefore, we consider their perspective are only limited to a certain scope. In this paper, a new taxonomy for the existing IoMT security principles is proposed as shown in Figure 2. It attempts to provide a comprehensive understanding of the IoMT security issues, considering all aspects of security principles, rather than just a few of them. These cyber security principles are intended to provide give organizations with a strategic direction on how to secure their systems and data against cyber threats. These cyber security concepts are classified into three categories: govern, protect, and detect. The following sections describe the scope of all these aspects.

VII. GOVERN

Govern refers to the policies, procedures, and processes that will be used to manage and monitor regulatory, legal, risk, operational, and environmental standards that should be

TABLE 1. Comparison of existing related survey papers.

Security Principles from Specific view								
	Risk Assessment		Authentication mechanism			Detection mechanism		
Ref	Threat Assessment	Variability Assessment	Impact Assessment	Physical Authentication	Based on cryptography	Based on BlockChain	Intrusion Detection	Malware Detection
[1]	No	No	No	High	Low	No	low	No
[25]	No	No	No	Low	Medium	No	Low	Low
[2]	No	No	No	Low	High	No	Low	No
[20]	M	No	yes	High	Low	No	Low	High
[26]	No	No	No	low	low	No	low	No
Our work	yes	yes	yes	High	High	High	High	High

included in the risk management process [27]. The emergence of IoMT has led to new security concerns and threats because IoMT devices are susceptible to various attacks over their open wireless connectivity [28]. It is more likely that, attackers may get elevated privileges, implant malicious code, or infect devices with malware due to the inability of these devices to detect these threats and lack of security measures, as well as poor security authentication mechanisms. Moreover, medical devices are vulnerable to botnets or zombie attacks which can further jeopardize human patients physically [29]. This can happen because the attacker can identify their medical information and medical conditions, therefore putting the patients' lives in danger. Therefore, it is crucial protect against threats by addressing the key IoMT security concerns. Furthermore, the implementation of IoMT systems in healthcare involves a number of risks, including the possibility of any medical device's transmitted data being manipulated and edited (Data Falsification), a negative impact on patients' health, and a negative impact on the institution's reputation (Personal Information Disclosure).

Besides, the lack of proper training on nurses and doctors also may alleviate the risk of jeopardizing patients' lives [20] as these could seriously result in permanent disabilities or fatalities. Therefore, it is critical to implement a risk management strategy prior to any security risks. By definition, risk management attempts to govern and estimate risk before it manifests itself [28]. Subsequently, a new risk assessment approach is required to estimate the security risks of IoMT threats. However, it is challenging. In general, the first step in establishing the appropriate security solutions for IoMT applications and communication protocols is to address threats in IoMT and analyze their associated risks [20].

A. IoMT-SPECIFIC RISK ASSESSMENT

In risk assessment, the threat, risk, and vulnerability analysis (TVRA) technique are implemented. The risk assessment was carried out in accordance with the ISO/IEC 27005 standard for handling information security risks [30]. TVRA is based on the probability of a specified attack, as well as the impact of the attack on system assets and associated threats. Furthermore, the TVRA approach identifies the threat agent that is attempting to compromise the system. Hence, TVRA outputs include risk measures for previously identified threats that can be estimated based on their probability and effect on the system [20], [31].

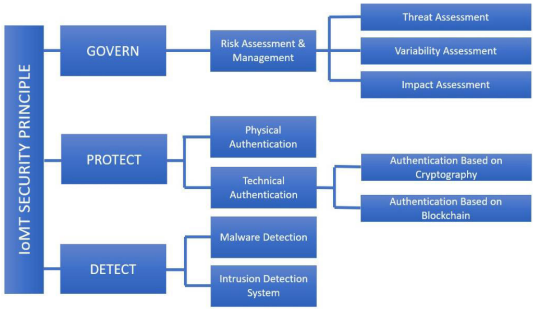


FIGURE 2. Taxonomy of IoMT Security Principles.

1) THREAT ASSESSMENT

According to [32] threat modeling is a standard practice for identifying cyber security threats. Threat models are extensively used to generate a catalogue of prospective threats based on a profile of potential malicious actors' motivations, techniques, and resources to precisely prevent attacks from exploiting system vulnerabilities. Various studies introduced several ways of modeling and assessing threats, most of which are based on well-established methodologies. Some of the most common approaches are presented here, with the applicability of each strategy defined by specific characteristics [32].

- Attack path approach: The threat model based on attack pathways considers how the attacker's mobility, capabilities, and motivation influence the probability of an attack. One significant finding is that all opponents of the IoMT paradigm must be strongly motivated. Bluetooth security risks are classified into three categories in [33] exposure, integrity, and disruption of service.
- Asset-based approach: in [34], an adversarial model with an asset-based strategy is also provided. The au- thors classify essential assets and the vulnerabilities that a threat agent can exploit to damage a system.
- STRIDE: The STRIDE architecture is used by Consumer Health Wearables (CHW), a subcategory of IoMT devices, to indicate system areas that need to be further secured [35]. In another study [36], the STRIDE methodology is used to investigate and classify an adversary model across mobile healthcare systems, including IoMT. It identifies a wide range of threats, including spoofing, tampering, repudiation, information leak, denial of service, and privilege elevation [32].

- Attack-tree approach: threat modeling requires the prioritization and categorization of various threats. A tree-based attack technique is described in [37], assessing a large number of related threats.

All adversaries of the IoMT paradigm must be extremely motivated. Other research categorizes threat agents differently. For example, in [38] threats are identified according to their capabilities, as well as the attackers' skills and resources. A threat-based medical cyber-physical systems (MCPS) concept is developed in [39],that partition users into four groups: trustworthy, trust- worthy but prone to errors, untrustworthy, and momentarily trustworthy. The study further describes why the attacker would violate patient privacy or have a direct impact on the patient's health. Reported in [40],the existing attacks that can be identified in health monitoring systems are described. The study in [41] proposed a system-theoretic process analysis (STPA) on an insulin pump device to detect accidents caused by security threats that are not protected by functional safety. In [30] used a threat-oriented analytical technique to assess the impacts of the attacks, a scenario-based analysis to determine the probability of threats occurring, and a composite analysis to select the most serious attack.

2) VULNERABILITY ASSESSMENT

A vulnerability assessment attempts to identify technical and/or non-technical security flaws that could be exploited by malicious users to create a security threat. The vulnerability assessment step is concerned with finding, quantifying, and prioritizing the multiple vulnerabilities in a system. The most common source of IoMT that enables vulnerability is, the medical equipment that is designed to be accessible for elderly people. Oftentimes, manufacturers frequently use poor authentication such as weak passwords for these types of systems. Furthermore, deploying robust encryption is not always achievable, and upgrading application environment firmware and evaluating the security of software APIs are not easy tasks for IoMT (such as implantable devices) [42]. Additionally, multiple levels should be considered in a full vulnerability assessment, including the devices, local and remote-control systems, and any other network-related services. Following that, various models for assessing the most common vulnerabilities for IoMT have been proposed.

For example, a graph model is provided in [43] for determining the parameters that would be used to evaluate the damage on both actors and flows of medical equipment. Other studies examine three major components of a system to assess network-based vulnerabilities: databases, application software, and web servers [44]. In [34] the researchers provide a vulnerability framework for IoMT based on assets. The proposed framework known as Common Vulnerabilities, and Exposures (CVE) are utilized to identify vulnerabilities, while a Common Vulnerability Scoring System (CVSS) is used as a metric system to analyze the weaknesses of implantable devices. The authors of [45] compile a dataset of IoMT- related and medical software vulnerabilities across a range of medical devices using the ICS-CERT and NVD databases. A CVSS score of (7) or (9) indicates that the vulnerabilities detected are of high severity. In [46] the authors presented a goal-oriented questionnaires security evaluation methodology for IoMT solutions that includes extensive and simple questions. The framework can be used to assess the needs of a variety of stakeholders, as well as solutions and architectures. The authors examine all documented IoMT-related vulnerabilities from NIST's National Vulnerability Database (NVD) and CVE Details to validate the proposed methodology.

3) IMPACT ASSESSMENT

Numerous methods have been proposed in the literature for evaluating and quantifying the impact of IoMT attacks. Typically, the most common attribute in impact evaluation and control is patient harm, while other studies consider the monetary worth of the impact [47]. As presented in [38] four categories may be recognized in this case based on the severity of the damage, including brand value loss, life risk, data disclosure, and monetary worth. Other research examines the impact of IoMT attacks in terms of confidentiality, integrity, and availability. Further [48] proposes four impact groups: patient safety, service personnel, or environment safety, maintenance, and cost. Meanwhile in [49], they analyzed on the ''human aspect'', placing the user in the situation and investigating their role in the accident dynamics.

VIII. PROTECT

It is the process of implementing security measures in control to mitigate security risks. Access control refers to a set of security measures that determines who should have access to a system or a part of a system. It is designed to restrict access to limit access to those who have been granted permission [50]. The fundamental security attributes of an effective access control system are confidentiality (preventing unauthorized disclosure of information), integrity (preventing resource modification without authorization), and availability (preventing resource modification without authorization and assuring access to resource by legitimate users when needed) [51]. A complete access control system covers three primary functions: authentication, authorization, and accountability [51]. One of the most significant features of security and privacy in IoMT is the authentication process [51]. Therefore, this survey is solely focused on the authentication mechanism. Authentication is the process of identifying and verifying users on a secure system. In a secure system, the user must first identify himself or herself, and the system will then verify the identification before authorizing the user access [52]. There have been other approaches proposed, including those based on who you are, what you have, what you know, where you are, and what you can do [53]. According to the literature, authentication mechanisms can be classified into two types: physical authentication and technical authentication [50].

A. PHYSICAL AUTHENTICATIONS

Physical access control (sometimes known as physical safeguarding) is a method of preventing or restricting physical access to resources. It is critical to have a strong identification and verification procedure in place to prevent unauthorized access to IoMT systems. Nowadays, the most effective solution is biometric systems [20].

Researchers are looking into the use of biometric intrinsic characteristics that are unique to the individuals in IoMT healthcare systems since it is more difficult to be exploited by attackers compared to short password frequently employed in smartwatches [2]. Biometric authentication systems are divided into two phases: enrollment and matching. During the enrollment phase, subjects register their raw biometric samples in the database, following which the recorded biometric samples are processed into a template or a feature vector and saved in the database. In the matching step, a similar approach is employed. The subject's sample will be validated only if it matches the templates or feature vectors of the claimed identity in the database. Otherwise, the system will deny the login attempt [2]. Identification and verification are two common functions performed by biometric-based security systems. Identification is the matching of a sample against all the samples in the database, whereas verification is the matching of an input sample to one person's samples in the database [2]. Several biometric approaches are required for identification and verification, which can be categorized into physical and behavioral biometric procedures [54]. Physical biometric measures can be used to protect and maintain the medical privacy of patients without exposing them to insider threats. This includes facial recognition, retina scans, and iris scans [20].

- One method that IoMT systems can utilize to authenticate users is facial recognition [55]. It can demonstrate a high rate of verification [56]. It performed identification based on facial structure of a person using a specialized digital video camera that identifies and measures the structure of the face such as the distance between the eyes, nose, and mouth. Therefore, it can distinguish between legal and unauthorized users by comparing scanned faces to permitted faces in the database. This technology can secure the medical system because it continuously scans the user's face while they are using it. This strategy, for example, can prohibit lower-level medical personnel from accessing patient data in the absence of a higher-level medical staff member who has been authorized but not logged out of the system [55].
- Fingerprint Recognition: This authentication verifies the identity of person using their unique fingerprint. It is one of the most used biometric authentication methods. Fingerprint techniques function by reading the image of the fingerprint. The extraction algorithm influences the performance of fingerprint sensors. These commonly used algorithms include Delaunay triangulation-based, pair-polar coordinate-based and minutia cylinder-code-based feature representation [55].
- Iris Scan: The pigmented tissue around a specific eye pupil is analyzed and scanned by an iris scan to see if it matches the stored data and, if so, whether access is granted or denied. Iris Scan has shown to be critical for both identification and verification due to its ability to generate accurate and precise measurements [20].
- Retinal Scan: A retinal scan is a biometric technology that uses unique patterns on the retina blood vessels to determine the identity of a person. According to [57], it is considered as very accurate and safe verification approach.
- Fingerprint Vein: Finger vein biometrics identifies people based on the vein patterns in their fingertips. The vein patterns of each individual are distinct. When it comes to finger vein image acquisition quality, the follow-up algorithm will have a substantial impact on the final accuracy; thus, a simple and effective acquisition equipment is necessary [58].
- Hand Geometry: Hand geometry is a biometric technology that identifies a person based on the shape of their hands. A camera is used to take a silhouette image of the hand. The biometric systems will analyze the hand measurements, such as palm size, hand shape, and finger dimensions [54]. The data is then compared to a collection of stored data to validate users. If there is a match, a specific member of the staff will be allowed access. Otherwise, access will be denied [20].

Table2 (retrieved from [59])summarizes the strengths and limitations of these physical biometric techniques. According to [58], multi-mode biometric identification, integrated three biometrics of face, fingerprint, and finger vein, which produced a high recognition rate and higher security characteristics. The use of this integrated system will be an unavoidable trend in the future development of the medical industry. Furthermore, based on [60] vital sign monitoring has revolutionized individualized medical care. Real-time vital sign monitoring [60], [61], [62]and [63] enables researchers to acquire a better understanding of a patient's physical status, and to assess and make decisions based on diagnosis and treatment data. This is beneficial for studying human diseases and developing preventive measures.

The support of wearable devices is intrinsically related to real-time vital sign monitoring and the realization of telemedicine [64]. Wearable devices such as rings, watches, and wristbands have made it easier to coordinate between medical staff and patients. Dao et al. [65] proposed an encrypted biomedical data with a multi-biometric encryption key technique and stored it in a safe fuzzy vault. The fingerprint data was used as the input for encryption, with the minutia of the fingerprint extracted and the input data encoded using a 16-bit technique.

B. TECHNICAL AUTHENTICATION

Technical authentication is a process of restricting or preventing access to an electronic resource. The goal of technical

TABLE 2. Comparison between different biometric techniques.

Biometric Techniques	Weaknesses	Strength
Face Recognition	need more hardware efficiency is poor.	broad use high accuracy. low froud.
Fingerprint Recognition	need more hardware hard to get good pictures.	broad use high accuracy. low cost.
Iris Recognition	need more hardware Costly	accurate
Retinal Scan	need more effort.	very secure Change is difficult replicate is difficult
Fingerprint Vein	difficult to acquire image.	noninvasive.
Hand Geometry Recognition	need more hardware	Easy to use low froud

authentication strategies is to restrict access only to those authorized individual [50]. In the IoMT literature, various methods of technical authentication mechanisms are presented. Thus, we review the most relevant authentication methods based on models that have been proposed.

1) AUTHENTICATION BASED ON CRYPTOGRAPHY

Cano and others [66] proposed the concept of dual signature (DS) in the elliptic curve digital signature algorithm (ECDSA). A Dual signature is not the same as a double signature; it is a technique for securely coupling two variables of distinct natures while keeping them anonymous to two independent entities [66]. It is also compatible with hardware implementations. The authors presented a novel approach for encryption and encoding to be used in IoMT based on the Advanced Encryption Standard (AES) [66]. They tested the performance of their system, which requires less time to execute encryption and encoding operations than traditional cryptography techniques. The author suggested a homomorphic encryption-based data fusion mechanism in [67] that used random numbers for real-identity perturbation to conceal test subjects' real identities during the data fusion process. Using a cipher block chaining algorithm, the authors in [68] created a safe approach for the proposed framework to convey sensitive information related to the patient's body from a sink node to medical institutions. Their suggested approach computes digital authentication utilizing private-public cryptography to validate the encrypted chain of the sensor data. The cryptography approach safeguards data privacy by obfuscating medical applications to produce computationally indistinguishable outputs. Kavitha et al. [69] established a formal model for addressing security concerns using the program obfuscation approach. Their indistinguishable inscrutable obfuscated medical data transfer can be deployed between standard-compliant equipment in a health service center or clinical center to eliminate fraud and internal human risks. The state-of-the-art obfuscation approach (GGH13) uses a variation of the multi-linear map. However, in such schemes, noise can be seen in each element of the matrix, indicating that the matrix is a full rank matrix with a probability of almost one (1), preventing the relationship between the matrix determinant and rank from being established. Jing and others [70] demonstrated that the class of attacks can be extended to show the obfuscator candidate, is vulnerable to a variation of attack when instantiated with the ADLP GES as proven on GGH13. Furthermore, the authors [71] presented a lightweight, robust, and physically secure Mutual Authentication and Secret Key (MASK) setup protocol for securing patients' sensitive health information. The proposed protocol employs lightweight cryptographic primitives such as the one-way hash function, nonce, PUF, and bitwise XOR operations. Wang and others [72] developed an efficient and private outsourced support vector machine training strategy (EPoSVM) for IoMT. They used partially homomorphic encryption (PHE) to keep data private even when it is used. The authors also converted a floating-point value to an integer, with the fractional part denoted by the least significant E bits. They then developed eight secure computation protocols to handle integers and floating-point numbers in this format. In [73], they have incorporated two apps in their system to represent security and compression functionalities, Advanced Encryption Standard (AES) and Lempel- Ziv compression (lzw), respectively. The AES from the Crypto++ package was selected that consists of a 128-bit block length and key lengths of 128, 192, and 256 bits. In their implementation, they used a 128-bit default block and key lengths. Both encryption and decryption are performed by the application. The program accepts an 11KB plain text file and converts it to an encrypted file. The final output text file is created by decrypting the encrypted file. Both files are compared to ensure a correct encryption and decryption. Their main contribution in [74] is a novel lightweight encryption technology for protecting the privacy of medical images of patients. In the suggested lightweight encryption algorithm, they used 256 bits for image encryption and then calculated the associated image's binary value using 16 sub- blocks of 16 bits. The suggested method ensures that medical data transmitted to healthcare facilities remains confidential and safe. OPenICE-lite was developed by [75] as a general-purpose IoMT middleware for safe and secure medical device interoperability. It is an open-source medical device interoperability platform that is lighter and more modular than OpenICE and adheres to the Integrated Clinical Environment (ICE) architecture. OpenICE-lite ensures security with end-to-end communication encryption and secure data logging features and made use of the lightweight Message Queuing Telemetry Transport (MQTT) protocol. Further, the authors employed the Transport Layer Security (TLS) protocol to provide

secure communication between any two MQTT clients. TLS is a popular communication protocol because it mixes symmetric and asymmetric encryption and offers excellent security guarantees if the keys are renewed regularly. Furthermore, OpenICE-lite can fight against most known information attacks, due to the TLS-augmented communication protocol such as eavesdropping and replay attacks. Replay attacks can be mitigated by including sequence numbers in the encrypted message. According to [76], they created a data-sharing scheme for the IoMT that is both safe and lightweight. Based on identity-based broadcast encryption, the approach ensures patient privacy and authorized access to shared data. Patients with health sensor devices collect and encrypt their data before uploading it to cloud servers for distribution. In addition, the patient specifies the identity of the user to acquire access. An entity known as Security-Mediator (SEM) helps patients in the development of blocks and block tags for subsequent integrity verification to verify cloud data (CD) integrity before sharing and reducing patient computation load. The authors presume that the SEM and CS are semi- trusted. In their scheme, the authors further proposed a Trusted Authority (TA) that is responsible for generating public and private system settings and issuing private keys to users based on their identities. In another work [77] the authors suggested Left Data Mapping (LDM) mechanism which translates each bit sequence to a corresponding shifted sequence, resulting in less deterioration, thus higher security for a given quantum of hidden data. The main goal of using LDM is to obtain high imperceptibility without sacrificing embedding capacity. The hidden secret message is divided into 3- bit chunks, each represented by a decimal value between 0 and 7. Additionally, the author devised a novel block checksum computation mechanism for localized tampering detection. A fragile watermark has also been used to assists in early tampering detection. Table 3 compares the existing Cryptography Mechanisms used in IoMT authentication. Table 3 compares the existing cryptography mechanisms used in IoMT authentication.

TABLE 3. Comparison of existing cryptography mechanisms.

Refer	Cryptography Mechanism	Advantages	Disadvantages
Ref	elliptic curve digital signature algorithm (ECDSA)	cryptographic protocol [78], Increasing the level of security shorter key lengths. [78]	large memory utilization, high computational power [79].
[80], [73]	Advanced Encryption Standard (AES)	need less time, flexibale [81]	too patents encryption .
[67] [72]	homomorphic encryption-based data fusion mechanism	apply operations on encrypted data, Data is securely stored in public clouds. [82]	high computational cost, high packet size [82]
[69]	Obfuscation Approach	varying degrees of data protection [83], high packet size	The original data set must be saved [83]
[77]	Left Data Mapping (LDM)	double layer security [84]	High computation cost. [84]

2) AUTHENTICATION BASED ON BLOCKCHAIN

Blockchain is an emerging technology that can provide a good solution for authentication and access services in IoMT enabled healthcare networks. It has cryptographic characteristics and a decentralized nature [85]. A blockchain is made up of a series of blocks, each of which is time-stamped and connected by cryptographic hashes distributed among network participants. Smart contracts can be coupled with blockchain to enable access control mechanisms for IoMT devices used in the healthcare area. Therefore, blockchain technology and the IPFS cluster are excellent for developing and managing distributed and decentralized infrastructures, as well as solutions for trust, integrity, authenticity, privacy, security, and storage in IoMT systems. The author described a new decentralized system based on IPFS cluster nodes and smart contracts in [85]. The Ethereum Ropsten network was used to design and deploy a consortium blockchain to protect the confidentiality of patient medical data. Their proposed method is divided into two parts: medical device components and IPFS cluster components. The medical device component is responsible for installing various medical devices in the IoMT to enable healthcare (specific patient's medical equipment) to interact via sensing and actuation. These medical devices generate data, which can later be transmitted over the blockchain network. The IPFS cluster component is responsible for ensuring the authentication of patients and medical devices. The IPFS cluster not only authenticates data but also ensures that it is stored securely in the IoMT system. The IPFS cluster nodes facilitates data synchronization for medical device authentication and authorization. In [86], BAKMP-IoMT is a revolutionary blockchain-based authentication and key management technique proposed by the authors for the IoMT environment. Furthermore, BAKMP-IoMT is designed with the private blockchain in mind. The stages of the BAKMP- IoMT are as follows: 1) predeployment, 2) key management, 3) user registration, 4) login, 5) authentication key agreement, 6) blockchain creation and addition, 7) password and biometric updating, and 8) dynamic IMD addition. Further, they used a cryptographic one-way hash function and bitwise XOR operations to make BAKMP- IoMT lightweight. According to [87], the authors presented the basics structure of blockchain and smart contracts, their applicability in the IoMT. They focused on the factors that contribute to the decentralization of smart contract adoption in IoMT. Besides, it also discusses the revolutionary architecture, as well as the benefits, issues, and future trends associated with their proposed integration. The decentralized Blockchain-based smart contracts for IoMT contain all the information linked to each patient transaction, including doctor details, prescription list and drug details, and pathology lab test reports. Each record holder serves as

a block, with data flowing from one to the next in a chain. In this chain, a hash serves as the starting point, and a hash is always added to the message with each move. In [88], the authors proposed a private blockchain- based system for medical data management. It uses Ethereum smart contracts to govern data access authorization between entities such as patients, hospitals, doctors, research organizations, and other stakeholders. The smart contract representation in medical records includes permissions, record owner- ship metadata, and data integrity. The medical record data is saved on an off-chain server, with a cryptographic hash of the record kept on the blockchain to ensure data integrity. Additionally, some publications, such as [89], have proposed modifying the consensus protocol to match the IoMT specificities. In [90], the authors presented a consortium blockchain-based architecture for securely recording data generated by IoMT while maintaining patient privacy. The blockchain functionality in the proposed architecture is defined by patient agent software (PA). It uses an Edge computing network for lightweight jobs and a cloud server for secure storage of massive amounts of health data. Smart contracts are used to manage health data in a variety of ways, including filtering clinically useless health data, triggering alarms in specific scenarios, transferring data to the cloud as needed, and classifying data. The authors of [91] presented a permission blockchain-based architecture for secure remote patient monitoring. They used Ethereum smart contracts to analyze data and send notifications to patients and healthcare providers. Instead of using the PoW consensus paradigm, they proposed the use of Practical Byzantine Fault Tolerance (PBFT). However, the proposed architecture does not address IoMT Blockchain integration issues. Conversely, the authors in [92] introduced a tailored blockchain-based infrastructure for IoMT devices. The proposed blockchain is private, therefore to join the network and send transactions, the nodes must be certificated. In such case, the POW consensus protocol was no longer used by the authors. They arranged encrypted data into blocks and stored the interconnected blocks in the cloud to deal with the enormous volume generated by IoMT devices. The hashes of blocks were retained on the blockchain to ensure tamper-proof storage. The authors utilized a 'lightweight privacy- preserving ring signature approach' that allows a set of nodes to participate in the data signature to ensure the anonymity and authenticity of the user. They then utilized a two-fold encryption approach in addition to a digital signature to secure data and ensure its integrity during transmission and storage. The key is encrypted using the receiver's public key, and the data is encrypted using the lightweight ARX technique. In [93] suggested the application of a blockchain-assisted safe data management framework (BSDMF) for health information based on the IoMT to securely transmit patient data while also improving scalability and data accessibility. The proposed BSDMF enables secure data transfer between personal servers and implantable medical devices, as well as between personal servers and the cloud. In the IoMT-based security framework, blockchain is employed to provide data transmission security and data management between linked nodes. Their suggested BSDMF approach achieves high accuracy, precision, average trust value, response time, and latency with minimal effort.

Furthermore, in [94] the authors investigated the advantages of blockchain-enabled IoMT, particularly in battling COVID-19. They specifically outline the architecture of blockchain-enabled IoMT and talk about the advantages it offers. Following that, they examine the IoMT-enabled blockchain responses to COVID-19 from five angles, including 1) pandemic origin tracing, 2) social isolation and quarantine, 3) smart hospitals, 4) medical data provenance, and 5) remote healthcare and telemedicine.

C. DETECT

Threat detection is the practice of analyzing the complete security ecosystem to identify any malicious activity that could compromise the network. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities. The majority of cutting-edge IoMT detection solutions are Intrusion Detection Systems (IDS) and Malware Detection Systems. Each mechanism will be discussed in detail in the following.

1) INTRUSION DETECTION SYSTEM

IDS is a type of security control that is commonly used to monitor and examine network/system traffic to detect anomalies and suspicious activities [71]. In [95], the authors utilized mobile agents for low-footprint intrusion detection in the medical environment. They also used machine learning and regression algorithms to detect network level intrusions and simulate hospital network topology to conduct IoMT experiments such as wireless body area networks (WABAN) and other DICOM network protocols used by connected devices such as ultrasound scanners and MRI machines. A wireless body area network is made up of wireless wearable or implanted devices that detect and transmit physiological data from patients to enable continuous patient monitoring, diagnosis, and therapy. They performed 72 independent simulations for each network type out of 216, resulting in an overall best and worst-case detection accuracy of 99.9% and 92.91%, respectively.

In [12] a novel IDS for health data prediction at the network's edge utilizing an intelligent experimental agent in an edge-centric edge concentrating on IoMT framework. Their proposed IDS technique is based on an empirical critical idea employed Swarm-NN strategy for detecting attacks and monitoring health data. The main objective of the proposed mode is to detect attacks during data transmission over a network, as well as to perform more efficient and accurate health data analysis at the network's edge. It was demonstrated that the Swarm- NN approach can effectively classified monitoring data with a 0.5% error rate. During the study, the suggested technique is tested on a realistic ToN-IoT data set that contains an estimated 99.5% of the attack styles in IoT

devices. Furthermore, the authors proposed the XSRU-IoMT model in IoMT networks for effective and timely detection of advanced attack vectors [96]. The proposed model exploits one-of-a-kind bidirectional simple recurrent units (SRU) that use the presence of skip connections to eliminate vanishing gradient concerns and accelerate recurrent network training. The evaluation results on the ToN-IoT dataset revealed that the proposed XSRU-IoMT model is more effective and superior to state-of-the-art compelling detection methodologies, meaning that it might be employed as a feasible actual deployment model for IoMT networks. The initial element of the proposed framework [13], consists of numerous smart health equipment that is interconnected via the internet and unique IP addresses, such as an intelligent pacemaker, intelligent wheelchair, intelligent glove and others. These devices periodically communicate sensitive data from the patient wearing the smart device, that is further stored the hospital's private cloud. The data may be accessible by intruder in variety of ways, even when it is stored in the cloud, during communication, or when transmitted to the doctor. Therefore, a deep neural network (DNN) was employed to develop a robust IDS to identify and forecast these unexpected cyber-attacks in the IoMT environment [13]. There are three procedures involved in the proposed model: pre-processing, dimensionality reduction, and classification. It was revealed that, the proposed DNN model outperforms conventional machine learning approaches with a 15% increase in accuracy and a 32% reduction in time complexity, enabling faster alarms trigger to avoid post-intrusion impacts on sensitive cloud data storage. The author in [97] presented a model for real-time seizure detection using an edge computing paradigm and the conventional kriging approach. Electroencephalogram (EEG) signals from patients were analyzed for fractal dimensional features and classified using the advised conventional kriging approach. The suggested model has perfect sensitivity, specificity, precision, and testing accuracy, with a training accuracy of 99.4%. In an edge computing setting, hardware implementation results in a mean detection delay of 85s. This is a novel study that employed the kriging approach for early detection in seizures. The authors in [98] proposed a cyberattack detection system powered by ensemble learning and fog-cloud architecture. The ensemble design integrates Decision Tree, Naive Bayes, and Random Forest as first- level individual learners. XGBoost used the categorization findings at the next level to detect normal and attack instances. The proposed model employs an accurate dataset ToN-IoT that is derived from a large-scale, diverse IoT networks. According to the experimental findings, the suggested framework can achieve a detection rate of 99.98%, a precision of 96.98%, and a decrease in false alarms.

2) MALWARE DETECTION

Malware is a catch-all phrase for any malicious program that enters a system without the user's permission. It poses a significant threat in today's digital world [99]. The author in [100] used a learning-based Deep-Q-Network technique to analyze and preserve the confidentiality and privacy of healthcare data. During this process, the system looks for intermediate attacks and malware to detect in an IoT- based healthcare system. The main goal of their work was to introduce a layered approach of Deep-Q-network for handling authentication, access control, and other types of rapid attacks on IoT-based apps for healthcare. The developed technique was employed to ensure the security, privacy, and dependability of the data. Therefore, the main objective of this project is to ensure security and privacy when accessing or sharing medical data over the IoT. The work in [101] introduced a novel deep multi-layer perceptive learning technique based on the blockchain dubbed Biserial Correlative Miyaguchi-Preneel Blockchain-based Ruzicka-Index Deep Multilayer Perceptive Learning (BCMPB-RIDMPL). The introduced model aims to enhance malware detection accuracy while minimizing its computation time. This study combined the advantages of deep-learning algorithms and blockchain technology. The BCMPB-RIDMPL technique used one input layer, three hidden levels, and one output layer to detect malware. The input layer received a large number of applications and malware features. The malware features were then transferred to the first hidden layer, where they were identified using point biserial correlation, which reduces the time required to identify the infiltration. The selected features were then transferred to the second hidden layer. In that tier, the hash value for each selected feature is generated using the Miyaguchi-Preneel cryptographic Hash-based blockchain. The hash values are stored in the blockchain after they have been generated. The classification was performed in the third hidden layers. This method increases the accuracy of malware detection. The experiments were conducted using Matthew's correlation coefficient, and the malware detection have been conducted on varying types of applications.

IX. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

The integration of medical equipment into the IoT have emerged in the development of IoMT since IoT devices have been used in a variety of medical settings. These devices can continuously monitor patients' health in the present, allowing them to be discharged from the hospital and strengthening their physical flexibility and mobility. In addition, IoMT applications are used by many healthcare organizations to improve patient care, manage prescriptions, monitor diseases, reduce human error, and improve patient satisfaction. However, the openness and dynamic architecture of IoMT have increased security and privacy concerns. Therefore, it is critical to address these security and privacy concerns by ensuring the security system is always up to date. Many studies has investigated measures on security and privacy, but there is still more to discover. Hence, this paper aims to provide a comprehensive survey on existing literature focusing on variety of security and privacy principles. These analysis includes different perspectives of research area such as risk management, IoMT system security, and methods for detecting security incidents or suspicious activity. In addition, we used a variety

of data sources to examine the unique needs and challenges of an IoMT system. The IoMT domain is still open for more future directions especially for academics, entrepreneurs, and vendors. The following are potential future research directions that could be used to improve the privacy and security of IoMT healthcare systems.

A. STEGANOGRAPHY

The system security and privacy based on IoMT is particularly critical for medical images such as X-rays, radiology, ultrasound, magnetic resonance imaging (MRI), and positron-emission tomography (PET), among other things. Following that, there will be a need to employ more efficient security mechanism for future implementation. The information security should not only be relied on encryption, but it should also focus on achieving an undetectable communication that is not visible to anyone in the communication channel. Alternatively, the use of steganography is introduced to avoid threats such as service repudiation or complete communication system disruption.

B. BLOCKCHAIN

The use of blockchain has been explored in previous literature for data authentication. However, its application came with many challenges. These challenges are presented as follows:

- Technical details are inadequate: integrating blockchain with the IoMT is difficult. Most of the previous systems failed to provide any technical information. Researchers are required to make clear all of the technical specifics pertaining to the blockchain's connection with IoMT.
- Abstractions in programming: The adoption of blockchain technology is difficult and requires thorough understanding of multi-disciplines. These includes the low-level discipline, such as managing IoMT devices and configuring blockchain to fulfill IoMT specifications, and to high level discipline, such as sharing, storing, and processing IoMT data. In this environment, it is critical to create an abstraction layer that hides all these difficulties to provide developers with new application programming interfaces (APIs) and middleware that make it simpler to build decentralized and secure healthcare applications using IoMT.
- Computational constraints: generating blocks in blockchain takes significant processing resources, which is difficult for IoMT devices with restricted capabilities.

C. DETECTION MECHANISM

In recent years, numerous machine learning-based network intrusion detection methods, such as in [13] and [12], have been presented. Moreover, the deep learning algorithms for disease diagnoses are becoming more popular in medical servers, therefore they are applicable to IoMT healthcare systems. Thus, researchers should consider the use of these approaches as solution to protect user privacy and system security.

X. CONCLUSION

IoMT is susceptible to cybersecurity attacks since attackers aim to gain unauthorized access to patients' confidential data and medical services. The main goal of this paper is to discuss the security and privacy principles across all IoMT domains to ensure a more complex, secure, and efficient system. Particularly, the paper examines on the IoMT research activities such as issues, challenges, and limitations of the IoMT system. The main contribution of this paper is the proposed novel taxonomy based on cybersecurity concepts such as govern, protect, and detect for IoMT security and privacy approaches. Following that, the paper thoroughly describes the security principles and classifies them based on how they are applied in the IoMT. Despite major efforts in the field, we discover that IoMT is still progressing. One example of a future research direction that could be used to improve the privacy and security of IoMT healthcare systems is steganography. Furthermore, the application of blockchain faces other problems, such as the integration of blockchain with IoMT challenging due to the large processing resources required for blocks construction.

REFERENCES

[1] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of Medical Things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.
[2] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.
[3] R. Hireche, H. Mansouri, and A.-S.-K. Pathan, "Security and privacy management in Internet of Medical Things (IoMT): A synthesis," *J. Cybersecurity Privacy*, vol. 2, no. 3, pp. 640–661, Aug. 2022.
[4] M. Morrison and G. Lăzăroiu, "Cognitive Internet of Medical Things, big healthcare data analytics, and artificial intelligence-based diagnostic algorithms during the COVID-19 pandemic," *Amer. J. Med. Res.*, vol. 8, no. 2, pp. 23–36, 2021.
[5] I. M. Shehabat and N. Al-Hussein, "Deploying Internet of Things in healthcare: Benefits, requirements, challenges and applications," *J. Commun.*, vol. 13, no. 10, pp. 574–580, 2018.
[6] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016.
[7] R. Chakravorty, "A programmable service architecture for mobile medical care," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOMW)*, Mar. 2006, p. 5.
[8] S. Salah, G. Maciá-Fernández, and J. E. Díaz-Verdejo, "A model-based survey of alert correlation techniques," *Comput. Netw.*, vol. 57, no. 5, pp. 1289–1317, Apr. 2013.
[9] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-based security recommendation for the Internet of Medical Things," *IEEE Access*, vol. 7, pp. 48948–48960, 2019.
[10] A. Mathew, "Threat intelligence and Internet of Medical Things (IoMT)," *Int. J. Eng. Trends Appl.*, vol. 7, no. 3, pp. 1–5, 2020.
[11] R. Moalla, H. Labiod, B. Lonc, and N. Simoni, "Risk analysis study of ITS communication architecture," in *Proc. 3rd Int. Conf. Netw. Future (NOF)*, Nov. 2012, pp. 1–5.
[12] 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 J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1969–1976, May 2021.

[13] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020.

[14] X. Li, B. Tao, H.-N. Dai, M. Imran, D. Wan, and D. Li, "Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic?" *Pervas. Mobile Comput.*, vol. 75, Aug. 2021, Art. no. 101434.

[15] N. V. Chawla and D. A. Davis, "Bringing big data to personalized healthcare: A patient-centered framework," *J. Gen. Internal Med.*, vol. 28, no. S3, pp. 660–665, Sep. 2013.

[16] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586, May 2014.

[17] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014.

[18] P. Kuila, S. K. Gupta, and P. K. Jana, "A novel evolutionary approach for load balanced clustering problem for wireless sensor networks," *Swarm Evol. Comput.*, vol. 12, pp. 48–56, Oct. 2013.

[19] E. Cavalcante, J. Pereira, M. P. Alves, P. Maia, R. Moura, T. Batista, F. C. Delicato, and P. F. Pires, "On the interplay of Internet of Things and cloud computing: A systematic mapping study," *Comput. Commun.*, vol. 89, pp. 17–33, Sep. 2016.

[20] J.-P.-A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing Internet of Medical Things systems: Limitations, issues and recommendations," *Future Gener. Comput. Syst.*, vol. 105, pp. 581–606, Apr. 2020.

[21] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of Medical Things (IoMT): Applications, benefits and future challenges in healthcare domain," *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017.

[22] R. P. Singh, M. Javaid, A. Haleem, R. Vaishya, and S. R. Ali, "Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," *J. Clin. Orthopaedics Trauma*, vol. 11, no. 4, pp. 713–717, 2020.

[23] G. Bigini, V. Freschi, and E. Lattanzi, "A review on blockchain for the Internet of Medical Things: Definitions, challenges, applications, and vision," *Future Internet*, vol. 12, no. 12, p. 208, Nov. 2020.

[24] F. Ellouze, G. Fersi, and M. Jmaiel, "Blockchain for Internet of Medical Things: A technical review," in *Proc. Int. Conf. Smart Homes Health Telematics*. Springer, 2020, pp. 259–267.

[25] 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)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4049, 2020.

[26] 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 *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 457–464.

[27] D. Nkomo and R. Brown, "Hybrid cyber security framework for the Internet of Medical Things," in *Blockchain and Clinical Trial*. Springer, 2019, pp. 211–229.

[28] S. Tarikere, I. Donner, and D. Woods, "Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G," *Bus. Horizons*, vol. 64, no. 6, pp. 799–807, Nov. 2021.

[29] G. W. Clark, M. V. Doran, and T. R. Andel, "Cybersecurity issues in robotics," in *Proc. IEEE Conf. Cognit. Comput. Aspects Situation Manage. (CogSIMA)*, Mar. 2017, pp. 1–5.

[30] M. Ngamboé, P. Berthier, N. Ammari, K. Dyrda, and J. M. Fernandez, "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)," *Int. J. Inf. Secur.*, vol. 20, no. 4, pp. 621–645, Aug. 2021.

[31] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[32] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," Carnegie Mellon Univ. Softw. Eng. Inst. Pittsburgh United, Tech. Rep., 2018.

[33] P. Luckett, J. T. McDonald, and W. B. Glisson, "Attack-graph threat modeling assessment of ambulatory medical devices," 2017, *arXiv:1709.05026*.

[34] K. Habib and W. Leister, "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures," in *Proc. 7th Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jul. 2015, pp. 1–5.

[35] J. Mnjama, G. Foster, and B. Irwin, "A privacy and security threat assessment framework for consumer health wearables," in *Proc. Inf. Secur. for South Afr. (ISSA)*, Aug. 2017, pp. 66–73.

[36] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2018, pp. 314–319.

[37] T. W. Manikas, D. Y. Feinstein, and M. A. Thornton, "Modeling medical system threats with conditional probabilities using multiple-valued logic decision diagrams," in *Proc. IEEE 42nd Int. Symp. Multiple-Valued Log.*, May 2012, pp. 244–249.

[38] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[39] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 114–119.

[40] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT smart health security threats," in *Proc. 19th Int. Conf. Comput. Sci. Its Appl. (ICCSA)*, Jul. 2019, pp. 26–31.

[41] T. Hayakawa, R. Sasaki, H. Hayashi, Y. Takahashi, T. Kaneko, and T. Okubo, "Proposal and application of Security/Safety evaluation method for medical device system that includes IoT," in *Proc. 7th Int. Conf. Netw., Commun. Comput. (ICNCC)*, 2018, pp. 157–164.

[42] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, "Risk assessment methodologies for the Internet of Medical Things: A survey and comparative appraisal," *IEEE Access*, vol. 9, pp. 40049–40075, 2021.

[43] H. Barkaoui, A. Guinet, and T. Wang, "Home health care vulnerability assessment using graph theory and matrix methods," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 4623–4629, 2017.

[44] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, p. 305, Jul. 2015.

[45] H. Debar, R. Beuran, and Y. Tan, "A quantitative study of vulnerabilities in the Internet of Medical Things," in *Proc. 6th Int. Conf. Inf. Syst. Secur. Privacy*, 2020, pp. 164–175.

[46] F. Alsubaei, A. Abuhussein, and S. Shiva, "A framework for ranking IoMT solutions based on measuring security and privacy," in *Proc. Future Technol. Conf.* Springer, 2018, pp. 205–224.

[47] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," Tech. Rep., 2018.

[48] K. Batbayar, M. Takacs, and M. Kozlovszky, "Medical device software risk assessment using FMEA and fuzzy linguistic approach: Case study," in *Proc. IEEE 11th Int. Symp. Appl. Comput. Intell. Informat. (SACI)*, May 2016, pp. 197–202.

[49] M. Catelani, L. Ciani, and C. Risaliti, "Risk assessment in the use of medical devices: A proposal to evaluate the impact of the human factor," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2014, pp. 1–6.

[50] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," *J. Med. Syst.*, vol. 41, no. 8, pp. 1–9, Aug. 2017.

[51] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.

[52] M. A. Alia, A. A. Tamimi, and O. N. AL-Allaf, "Cryptography based authentication methods," in *Proc. WCECS*, San Francisco, CA, USA, Oct. 2014, pp. 22–24.

[53] R. Gorrieri and P. Syverson, "Varieties of authentication," in *Proc. 11th IEEE Comput. Secur. Found. Workshop*, Jun. 1998, pp. 79–82.

[54] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools Appl.*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018.

[55] 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 Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2020.

[56] J. D. Woodward, C. Horn, J. Gatune, and A. Thomas, "Biometrics: A look at facial recognition," Rand Corp Santa Monica CA, Tech. Rep., 2003.

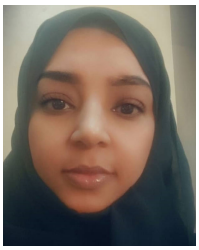
[57] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
[58] Y. Xin, L. Kong, Z. Liu, C. Wang, H. Zhu, M. Gao, C. Zhao, and X. Xu, "Multimodal feature-level fusion for biometrics identification system on iomt platform," *IEEE Access*, vol. 6, pp. 21418–21426, 2018.
[59] H. Hamidi, "An approach to develop the smart health using Internet of Things and authentication based on biometric technology," *Future Gener. Comput. Syst.*, vol. 91, pp. 434–449, Feb. 2019.
[60] S. Banou, M. Swaminathan, G. R. Muns, D. Duong, F. Kulsoom, P. Savazzi, A. Vizziello, and K. R. Chowdhury, "Beamforming galvanic coupling signals for IoMT implant-to-relay communication," *IEEE Sensors J.*, vol. 19, no. 19, pp. 8487–8501, Oct. 2018.
[61] Z. Ning, K. Zhang, X. Wang, L. Guo, X. Hu, J. Huang, B. Hu, and R. Y. K. Kwok, "Intelligent edge computing in Internet of Vehicles: A joint computation offloading and caching solution," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2212–2225, Apr. 2020.
[62] F. Lamonaca, E. Balestrieri, I. Tudosa, F. Picariello, D. L. Carni, C. Scuro, F. Bonavolonta, V. Spagnuolo, G. Grimaldi, and A. Colaprico, "An overview on Internet of Medical Things in blood pressure monitoring," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2019, pp. 1–6.
[63] W. Young, J. Corbett, M. S. Gerber, S. Patek, and L. Feng, "DAMON: A data authenticity monitoring system for diabetes management," in *Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 25–36.
[64] Y. Sun, H. Qiang, J. Xu, and G. Lin, "Internet of Things-based online condition monitor and improved adaptive fuzzy control for a medium-low-speed maglev train system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2629–2639, Apr. 2020.
[65] V. H. Dao, Q. D. Tran, and T. H. L. Nguyen, "A multibiometric encryption key algorithm using fuzzy vault to protect private key in BioPKI based security system," in *Proc. IEEE RIVF Int. Conf. Comput. Commun. Technol., Res., Innov., Vis. Future (RIVF)*, Nov. 2010, pp. 1–6.
[66] M.-D. Cano and A. Cañavate-Sanchez, "Preserving data privacy in the Internet of Medical Things using dual signature ECDSA," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jun. 2020.
[67] H. Lin, S. Garg, J. Hu, X. Wang, M. Jalil Piran, and M. S. Hossain, "Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15683–15693, Nov. 2020.
[68] T. Saba, K. Haseeb, I. Ahmed, and A. Rehman, "Secure and energy-efficient framework using Internet of Medical Things for e-healthcare," *J. Infection Public Health*, vol. 13, no. 10, pp. 1567–1575, Oct. 2020.
[69] D. Kavitha and C. Subramaniam, "Security threat management by software obfuscation for privacy in Internet of Medical Thing (IoMT) application," *J. Comput. Theor. Nanoscience*, vol. 14, no. 7, pp. 3100–3114, Jul. 2017.
[70] Z. Jing, C. Gu, Y. Li, M. Zhang, G. Xu, A. Jolfaei, P. Shi, C. Tan, and X. Zheng, "Security analysis of indistinguishable obfuscation for Internet of Medical Things applications," *Comput. Commun.*, vol. 161, pp. 202–211, Sep. 2020.
[71] M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, "A lightweight and robust secure key establishment protocol for Internet of Medical Things in COVID-19 patients care," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 2020.
[72] J. Wang, L. Wu, H. Wang, K.-K.-R. Choo, and D. He, "An efficient and privacy-preserving outsourced support vector machine training for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 458–473, Jan. 2020.
[73] A. Limaye and T. Adegbija, "HERMIT: A benchmark suite for the Internet of Medical Things," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4212–4222, Oct. 2018.
[74] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.-H.-A. Hashim, S. Habib, M. Islam, S. Alyahya, M. M. Ahmed, S. Kamil, and M. A. Hassan, "Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021.
[75] R. Ivanov, H. Nguyen, J. Weimer, O. Sokolsky, and I. Lee, "OpenICE-lite: Towards a connectivity platform for the Internet of Medical Things," in *Proc. IEEE 21st Int. Symp. Real-Time Distrib. Comput. (ISORC)*, May 2018, pp. 103–106.
[76] X. Lu and X. Cheng, "A secure and lightweight data sharing scheme for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 5022–5030, 2020.
[77] S. A. Parah, J. A. Kaw, P. Bellavista, N. A. Loan, G. M. Bhat, K. Muhammad, and V. H. C. de Albuquerque, "Efficient security and authentication for edge-based Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15652–15662, Nov. 2020.
[78] W. El Sobky, S. Hamdy, and M. H. Mohamed, "Elliptic curve digital signature algorithm challenges and development stages," *Int. J. Innov. Technol. Exploring Eng.*, vol. 10, no. 10, pp. 121–128, Aug. 2021.
[79] J. Doerner, Y. Kondi, E. Lee, and A. Shelat, "Secure two-party threshold ECDSA from ECDSA assumptions," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 980–997.
[80] I. S. Farahat, A. S. Tolba, M. Elhoseny, and W. Eladrosy, "A secure real-time internet of medical smart things (IOMST)," *Comput. Electr. Eng.*, vol. 72, pp. 455–467, Nov. 2018.
[81] O. G. Abood and S. K. Guirguis, "Enhancing performance of advanced encryption standard for data security," *Int. J. Eng. Andin. Syst.*, vol. 2, no. 11, pp. 32–38, 2018.
[82] G. Peralta, R. G. Cid-Fuentes, J. Bilbao, and P. M. Crespo, "Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges," *Electronics*, vol. 8, no. 8, p. 827, Jul. 2019.
[83] D. E. Bakken, R. Rarameswaran, D. M. Blough, A. A. Franz, and T. J. Palmer, "Data obfuscation: Anonymity and desensitization of usable data sets," *IEEE Security Privacy*, vol. 2, no. 6, pp. 34–41, Nov. 2004.
[84] M. S. Yaraziz and H. Bolhasani, "Edge computing applications for IoT in healthcare: A systematic literature review," Tech. Rep., 2021.
[85] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and ipfs technology," *J. Supercomput.*, vol. 77, no. 8, pp. 1–40, 2021.
[86] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of Medical Things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.
[87] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain based smart contracts for Internet of Medical Things in e-healthcare," *Electronics*, vol. 9, no. 10, p. 1609, Oct. 2020.
[88] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, p. 94, Jan. 2020.
[89] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, "A forensics-by-design management framework for medical devices based on blockchain," in *Proc. IEEE World Congr. Services (SERVICES)*, Jul. 2019, pp. 35–40.
[90] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged decentralized IoT eHealth framework," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100159.
[91] K. Griggs, O. Ossipova, C. Kohlios, A. Baccarini, E. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, 2018.
[92] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.
[93] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Pers. Ubiquitous Comput.*, vol. 2021, pp. 1–14, Jun. 2021.
[94] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled Internet of Medical Things to combat COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 52–57, Sep. 2020.
[95] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020.
[96] 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 Gener. Comput. Syst.*, vol. 127, pp. 181–193, Feb. 2022.
[97] I. L. Olokodana, S. P. Mohanty, E. Kougianos, and O. O. Olokodana, "Real-time automatic seizure detection using ordinary Kriging method in an edge-IoMT computing paradigm," *Social Netw. Comput. Sci.*, vol. 1, no. 5, pp. 1–15, Sep. 2020.
[98] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.

[99] P. Vinod, R. Jaipur, V. Laxmi, and M. Gaur, "Survey on malware detection methods," in *Proc. 3rd Hackers' Workshop Comput. Internet Secur. (IITKHACK)*, 2009, pp. 74–79.
[100] P. M. Shakeel, S. Baskar, V. R. S. Dhulipala, S. Mishra, and M. M. Jaber, "Retraction note: Maintaining security and privacy in health care system using learning based deep-Q-networks," *J. Med. Syst.*, vol. 46, no. 6, pp. 1–10, Jun. 2018.
[101] A. S. Alotaibi, "Biserial Miyaguchi–Preneel blockchain-based Ruzicka-indexed deep perceptive learning for malware detection in IoMT," *Sensors*, vol. 21, no. 21, p. 7119, Oct. 2021.

TAQWA AHMED ALHAJ received the B.Sc. (Hons.) and M.Sc. degrees in computer science from the Faculty of Mathematical and Computer Sciences, University of Khartoum, Sudan, in 2010 and 2012, respectively, and the Ph.D. degree from the Faculty of Computing, University Technology Malaysia (UTM), Malaysia, in 2019. She is currently a Postdoctoral Fellow with the Institute for Artificial Intelligence and Big Data (AIBIG), Universiti Malaysia Kelantan (UMK). Her current research interests include artificial intelligence, data, information security, intrusion detection systems, the IoT, and SDN networks.

SETTANA MOHAMMED ABDULLA received the B.Sc. degree (Hons.) in computer science from the Department of Mathematical Sciences, University of Khartoum, Sudan, in 2013, and the master's degree in computer science from the University of Khartoum, in 2015. She has many publications in field of information security. Her current research interests include information security, the IoT, image processing, cloud computing, and web base design.

MOHMMED ABDULLA ELSHEKH IDERSS received the B.Sc. (Hons.) and M.Sc. degrees in computer science from the University of Khartoum, Sudan, in 2010 and 2015, respectively. His current research interests include information security, cloud computing, and artificial intelligence.



ALAA ABDALATI AHMED ALI received the B.Sc. degree (Hons.) in computer science from the Department of Mathematical Sciences, University of Khartoum, Sudan, in 2013, and the master's degree in business intelligence–information technology from the University of Khartoum, in 2019. Her current research interests include business intelligence, the IoT, data scientist, and machine learning.

FATIN A. ELHAJ received the B.S.C. and M.S.C. degrees in computer science from the University of Khartoum, in 2005 and 2009, respectively, and the Ph.D. degree from the Faculty of Computing, University Technology Malaysia, in April 2018. Her research interests include encompasses the area of digital signal processing, image processing, and design of new algorithms to improve the effectiveness of searching and mining new knowledge from various kinds of datasets.

MUHAMMAD AKMAL REMLI received the master's and Ph.D. degrees in computer science from the Universiti Teknologi Malaysia, in 2014 and 2018, respectively. He was with the Universiti Malaysia Pahang, from 2018 to 2020. He joined the Institute for Artificial Intelligence and Big Data (AIBIG), Universiti Malaysia Kelantan (UMK), in early 2020, as a Fellow Researcher. He is currently the AIBIG's Director and also a Senior Lecturer with the Department of Data Science, UMK. His main research interests include artificial intelligence, data science, business intelligence, and computational systems biology.

LUBNA ABDELKAREIM GABRALLA received the B.S.C. and M.Sc. degrees in computer science from the University of Khartoum and the Ph.D. degree in computer science from the Sudan University of Science and Technology, Khartoum, Sudan. She is currently an Associate Professor with the Department of Computer Science and Information Technology, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her current research interests include soft computing, machine learning, and deep learning. She became a Senior Fellow (SFHEA), in 2021.