



REVIEW

A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things

Mohammad Kamrul Hasan¹  | Taher M. Ghazal^{1,2} | Rashid A. Saeed³  |
 Bishwajeet Pandey⁴ | Hardik Gohel⁵ | Ala' A. Eshmawi⁶ | S. Abdel-Khalek^{7,8} |
 Hula Mahmoud Alkhasawneh⁹

¹ Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Kuala Lumpur, Malaysia

² School of Information Technology, Skyline University College, Sharjah, UAE

³ Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

⁴ Gyancity Research Consultancy Pvt Ltd, Motihari, India

⁵ Department of Computer Science, University of Houston-Victoria, Victoria, Texas, USA

⁶ Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

⁷ Mathematics and Statistics Department, College of Science, Department of Mathematics, College of Science, Taif University, Taif, Saudi Arabia

⁸ Department of Mathematics, Faculty of Science, Sohag University, Sohag, Egypt

⁹ College of Computer Science and Engineering, University of Ha'il, Hail, Saudi Arabia

Correspondence

Mohammad Kamrul Hasan, Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Kuala Lumpur, Malaysia.

Email: hasankamrul@ieeee.org, mkhasan@ukm.edu.my

[Correction added on 25-November-2021, after first online publication: Author name is corrected from Taher M. Ghazel to Taher M. Ghazal in this version of paper.]

Abstract

The recent advancements of Internet of Things (IoT) embedded systems, wireless networks, and biosensors those have assisted in the rapid development of implanting wearable sensors are reviewed here. The applications of the internet of medical things (IoMT) that has gained major attention as an ecosystem of connected clinical systems, computing systems, and medical sensors geared towards improving the quality of healthcare services are also reviewed here. The 5G based AI technology can revolute the perception of healthcare and lifestyle. In light of the importance of IoT platforms and 5G networks, the purpose of this proposed research work is to identify threats that could undermine the integrity, privacy, and security of IoMT systems. Also, the novel blockchain-based approaches that can help in improving the confidentiality of IoMT network. It has been discovered that IoMT is vulnerable to various types of attacks, including denial of service (DoS), malware, and eavesdropping attack. In addition, IoMT is exposed to various vulnerabilities, such as security, privacy, and confidentiality. Despite multiple security threats, there are novel cryptographic techniques, such as access control, identity authentication, and data encryption that can help in improving the security and reliability of IoMT devices.

1 | INTRODUCTION

The recent advancement in semiconductor and related technologies includes microelectron mechanical sensors and systems, the internet-of-things (IoT) has gained notable attention.

The smart devices make use of artificial intelligence (AI) in order to make intelligent predictions. However, as mentioned in [1], to ensure that these devices effectively use federated learning – an ideal collaboratively learning for IoMT devices, they are required to be connected to a wireless communication

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial License](https://creativecommons.org/licenses/by-nc/4.0/), which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

© 2021 The Authors. *IET Communications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology

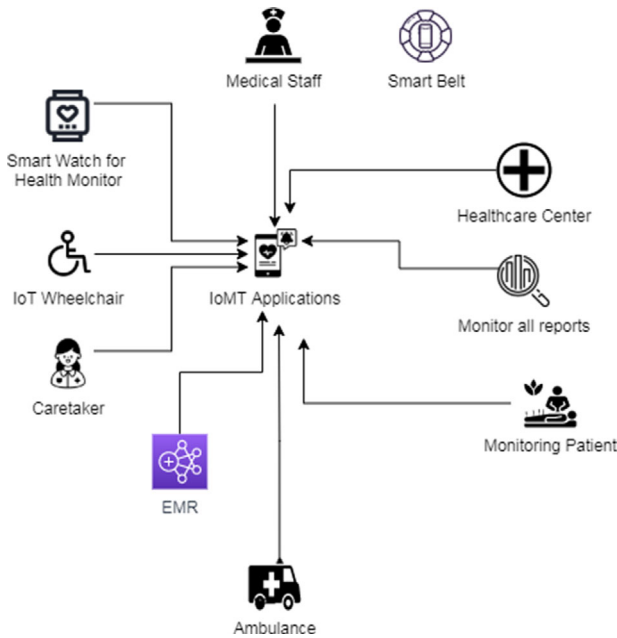


FIGURE 1 Application of Medical Internet of Things for healthcare services

network to perform different heavy computational task. For this purpose, the support needed for intelligent medical devices is only possible with 5G, or beyond communication technology. The use of these technologies, as discussed by [2] are not only limited to smartphones, but they also have a wide range of applications, ranging from smart watches to healthcare monitoring. While the use of 5G network design can significantly improve the cost, flexibility, and capability of the IoMT network [3]. Despite the high requirements, 5G networks will use terahertz signal for transmission, the data rate of more than 1TBPS, and will follow 3-dimensional communication structure – frequency, space, and time – instead of 2D as found in 5G networks. This will provide a strong architecture for medical IoT devices with broader and deeper coverage.

Block-chain enabled IoT is an evolving technological paradigm that has connected billions of smart objects, which has further resulted in the creation of smart ecosystems, such as smart cities, smart factories, smart health, smart vehicular network, smart home, and smart grids. One of the most crucial areas in adopting technologies to provide ubiquitous and real-time services in the healthcare sector [4, 5]. Under the umbrella of IoT, a broad range of entities, such as machines, people, and things are interconnected into data space anywhere, and at any time. The rise and evolution of IoT are dynamically changing the healthcare industry by introducing IoMT, where medical devices are interlinked through a global network that can be accessed by anyone, anywhere, and anytime (see Figure 1).

This makes IoT the next milestone in the technological growth of the world, with it having an expansion rate of over 270% [6–8]. However, despite having a substantial role in transforming the future of smart cities, the increasingly pervasive, dense, and invisible collection, dissemination, and processing of data in the course of people’s private lives are giving rise to seri-

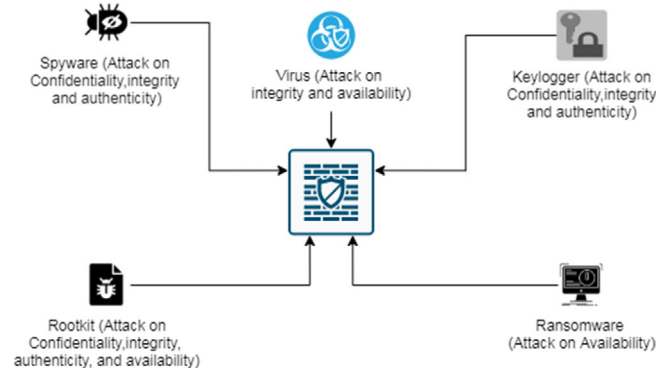


FIGURE 2 Various security vulnerabilities in Medical Internet of Things

ous privacy concerns [9–11]. In particular, IoMT devices, such as implanted sensors and medical wearable that constitute the major rudimentary components of the IoMT edge network are at risk due to various types of cybersecurity threats, and thereby, they pose a substantial risk to the safety and privacy of the patient. The dynamic and heterogeneous nature of IoT devices amplifies the possibilities of cyber exploits significantly that may cause data-injection attacks, Denial of Service (DoS), Distributed Denial of Service (DDoS), sophisticated botnet attacks, and advance persistent attacks that can jeopardize the confidentiality and availability of available processes, data, or even cause whole ecosystem chaos [12–14]. Unauthorized access to patient’s medical data can cause potential harm in terms of prescribing incorrect medical prescriptions that may further lead to health hazards or even potential deaths. Hence, besides leveraging huge benefits, IoMT is vulnerable to cyber threats, such as malicious bot proliferation, identity theft, phishing, and keylogging, which ultimately makes the biomedical domain a critical area of research (see Figure 2). In addition to potential cybersecurity threats, the digital landscape of IoMT is also susceptible to hacking approaches that can sabotage physical security [15, 16]. Thus, the fact that security is a crucial factor that depends on the medical device’s reliability, for the successful integration of IoMT technology into healthcare systems, there is a need for a security mechanism that can safeguard the security of IoMT network [17, 18]. To this end, the primary step is to identify potential and existing threats to the IoMT network. As IoMT devices have similar technical characteristics and capabilities to that of IoT devices, existing attacks that threaten IoT networks can also be considered as threats that can inflict damage to IoMT devices.

Finally, this paper will highlight the significance of modern solutions that can mitigate cybersecurity threats.

2 | BACKGROUND STUDY

A growing number of organisations have realized that information security risks can negatively impact business continuity and public image while also creating problems with legal authorities in the event of non-compliance. These risks can also result in financial loss and negatively impact relationships with customers, partners, and the satisfaction of those relationships.

“Information security is the safeguarding of data and the essential components within it,” Information security is characterised by three main characteristics: Confidentiality, integrity, and availability. It’s important to maintain confidentiality because it limits who has access to information. The integrity of information refers to how complete and unaltered it is. The availability property makes data accessible to users or other systems [110].

For a few years now, the internal threat has been a hot topic in information security. However, the available data on this subject is depressing. 50 percent of those polled said they expected to suffer financial losses only from external attacks in 2008, not from insider abuse. However, 44 percent of those polled have admitted to having been victims of insider abuse in 2008, making it the second most common form of information security fraud after viruses. Ernst and Young’s most recent survey (2009) also reveals that internal risk is high, with 25% of respondents reporting an increase in internal attacks and 13% reporting an increase in internally perpetrated fraud.

It is possible that an employee, ex-employee, partner or client with authorised access to an organization’s assets will use that access in a way that compromises the organization’s information security, which is referred to as an “internal threat”. Internal threat is a concern for all organisations, as employee behaviour or ignorance can lead to incidents of varying severity, ranging from a few lost work hours to negative publicity or financial damage, and thus the organisation may not survive. Internal threat may be more important than external threat, according to some researchers, but not every company sees its employees as a serious threat factor [111].

Fear of the unknown makes humans distrust their coworkers as potential criminals. Our fear of hackers can cause us to react inappropriately when dealing with information security issues because those we know and trust (such as IT support staff) have no reason to fear us. Contrasting employees with those without physical or logical access rights, insiders have a greater opportunity to compromise the information security of the company.

When supervisors are suspicious of their employees and view them as criminals, too strict requirements can lead to a culture of ignorance that allows for the circumvention of regulations and fosters dissatisfaction. It’s important to strike a balance between security and usability, but different aspects of threats, risks, countermeasures, and people should be taken into account within the organisation. As a matter of fact, many firms face the dilemma of protecting information that must be shared with employees in order to carry out or support business processes.

3 | REVIEW METHODS

The research paper can use the qualitative, quantitative, and mixed approach. In a qualitative approach, the research focuses on an in-depth and detailed study of the theoretical data that is usually collected to describe or state a phenomenon through open-ended tools. However, when a quantitative approach is selected, the research is focused on numerical or statistical data collected to either prove any hypothesis or evaluate associations

between the selected variables. A research approach must be chosen as per the pre-defined objectives. Therefore, to accomplish the objectives of the current study, this research adopted a quantitative approach.

The selection of a suitable research approach provides the base for the research; however, the data collection stage is necessary for collecting the required data from the sources that could be analysed for interpretation and statistical results. There are generally two data sources that provide data for the research, that is, primary and secondary data sources. Primary data sources are usually based on the participants that are selected for acquiring first-hand and original data that is specifically directed towards the research objective. However, companies usually outsource such researches to research agencies due to the time and cost constraints. On the other hand, secondary data sources may be in the form of literature sources such as journal articles, website articles, books, conference proceedings or annual reports of organizations. It has been established that this information comprises the risk of being either irrelevant or outdated. However, secondary research is usually considered to be cost and time effective and minimizes ethical risks. In this regard, data is collected from sources such as IEEE, Springer and Elsevier journals.

4 | VULNERABILITIES IN IOMT NETWORKS

There are three major vulnerabilities in IoMT networks, that is, security, privacy, and confidentiality discussed in the following subsections.

4.1 | Security

Due to the dependence on open wireless communication, IoMT devices are vulnerable to network/wireless attacks [19]. An adversary can intercept and eavesdrop on outgoing and incoming data due to the absence of security measures that IoMT devices suffer because of design or weak security authentication measures [20, 21]. Moreover, since most IoMT devices are incapable of detecting and preventing attacks, skilled attackers can bypass the security to gain unauthorized access to patient’s data [22, 23]. As a consequence, attackers can exploit elevated privileges while infecting devices with malicious codes or malware [24]. This is apparent in the study of [25], where the authors demonstrated how medical devices are vulnerable to zombies or botnet attacks. For example, an attack can logically change or manipulate drug dose that can lead to serious health implications or a patient’s death [26]. Consequently, since most IoMT devices take advantage of blockchain technology, an adversary can identify the patient’s record on the blockchain network [27, 28]. Moreover, in healthcare systems, medical data are prone to fabrication that can lead to the wrong administration of medication and prognosis of the patient that can further result in an allergic response [29, 30, 31]. Due to security vulnerabilities, attackers can also send fake medical alerts and cause substantial financial losses.

Healthcare facilities, on the other hand, must now consider cyber-security a strategic issue [107]. Health care facilities are a prime target for hackers due to the outdated deference, shoddy information systems, and general lack of IT management in hospitals. They use ransomware to cripple the systems, sell patient data to the highest bidder, threaten to make private information public, and cut off the power to the hospitals.

In [108], researchers looked at SVM classification while keeping security in mind. It was possible to secure the training set in many other ways before. One approach reveals the set rate to the other users, while the other approach hides it from the users. Both approaches assume that the final classifier is safely stored by a reputable third party and do not address the protection of SVM after learning.

4.2 | Privacy

The data collected from IoMT devices can reveal sensitive information regarding the habits of a patient [28]. For example, as mentioned by [6], signals transmitted from the sensors that are used to report the condition of a patient can reveal the device's medical functions. Likewise, with passive attacks like traffic analysis, attackers can either dissolve or gather information about the identity of patients, in addition to confidential and sensitive information [32, 33]. More importantly, as discussed by [34–36] attacks, such as man-in-the-middle (MitM) can sabotage the integrity and privacy of IoMT networks by interposing in the communication to alter the exchange data between two parties without being noticed. For example, the collected medical data can be sent to a remote server where attackers can modify and intercept the medical data to compromise their privacy. Furthermore, since unauthorized information storage is vulnerable to integrity, privacy, and data security attacks, researchers like [37–39] have rendered privacy and security issues a major threat to user privacy and data confidentiality. This is quite apparent in IoMT devices because it lacks a reliable authentication mechanism [40, 41]. Consequently, the lack of network access control and data encryption allow attackers to breach user privacy via eavesdropping.

The privacy support process in a trained SVM could also be described using [109], which is another method. Although this approach does not accept Gaussian function roles, it can only be used with Gaussian Kernels the final SVM has the potential to leak information about the final classifying types even though it offers privacy. As a result, this method has a low accuracy rate. When in fact the main goal should be to release a final classifier while protecting patients' support vectors' privacy, most solutions concentrated on medical classifiers. If they create an SVM classifier, they will be able to create the support vectors needed to practically rebuild the subject's biometric data. It's because of this that these systems don't work. SVM authentication matching systems should be developed with a focus on preventing the disclosure of sensitive data from sample classifications.

4.3 | Confidentiality

The data collected from IoMT devices can reveal sensitive information regarding the habits of a patient [42, 43]. For example, as mentioned by [6], signals transmitted from the sensors that are used to report the condition of a patient can reveal the device's medical functions. Likewise, with passive attacks like traffic analysis, attackers can either dissolve or gather information about the identity of patients, in addition to confidential and sensitive information [44]. More importantly, as discussed by [34], attacks, such as man-in-the-middle (MitM) can sabotage the integrity and privacy of IoMT networks by interposing in the communication to alter the exchange data between two parties without being noticed. For example, the collected medical data can be sent to a remote server where attackers can modify and intercept the medical data to compromise their privacy [45]. Furthermore, since unauthorized information storage is vulnerable to integrity, privacy, and data security attacks, researchers like [37, 38, 46] have rendered privacy and security issues a major threat to user privacy and data confidentiality. This is quite apparent in IoMT devices because it lacks a reliable authentication mechanism [47, 48]. Consequently, the lack of network access control and data encryption allow attackers to breach user privacy via eavesdropping.

5 | ATTACK TYPES IN IOMT

The attacks such as DoS, Malware and Eavesdropping attack has been identified, the detail discussions are as below:

5.1 | DoS attack

The recent increase in cyberattacks and identity theft have made the internet a daunting place [49]. Such attacks can affect the biomedical domain as of today's economic, social, and medical infrastructure heavily dependent on computer networks and information technology (IT) [50, 51]. Over the decades, cyber-security practitioners have discovered multiple types of cyber threats that could potentially jeopardize information security. According to a recent report [52], malware, eavesdropping, and Denial of Service (DoS) attacks are amongst the most dangerous cybersecurity threats that can compromise IoMT security [53]. In a DoS attack, a malicious attacker attempt to clog the computing resources of a computer or wearable device by sending a significant number of requests [54]. The study of [55] argues that these attacks are conducted in different ways. For example, one single attacker machine can overwhelm a victim's machine by transmitting a substantial number of network packets – which often appears to be legitimate [56]. This activity is usually done to bypass network security. On the other hand, an adversary can also use multiple machines to launch simultaneous attacks in a distributed style. Moreover, as discussed by [20], DoS attacks disrupt the accessibility of a given medical IoMT device or system to prevent authorized patients from getting

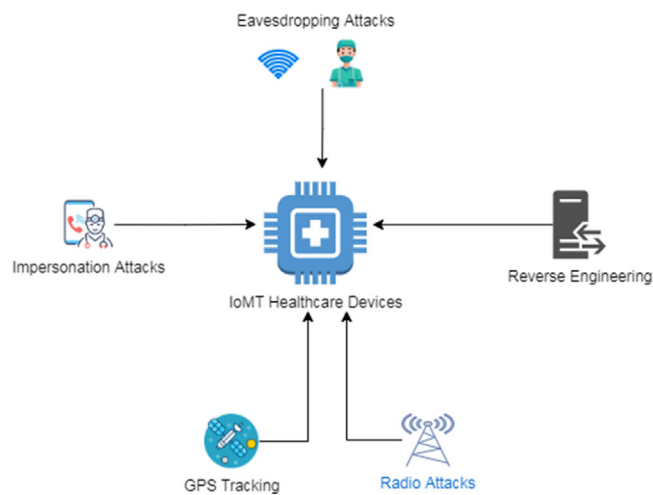


FIGURE 3 Attacks on electronic systems [41]

medication and preventing doctors and nurses from accessing medical records.

5.2 | Malware attack

IoMT devices are also prone to different types of malware, including botnets, backdoor, spyware, viruses, worms, Trojans, and more [57]. Studies like [58, 59] analysed the phenomenon and proclaim that malware attacks automatically spread throughout the network by exploiting known or unknown vulnerabilities [60]. These attacks not only threaten the integrity and confidentiality of IoMT devices, but they are also capable of shutting down any network server through DDoS attacks [61, 62]. This can forcefully open a backdoor to a given medical system or device [63, 64]. Besides, exploiting the security gap can also lead to unauthorized access to medical records, disclosure, IoMT devices, or deletion of patient's information [20]. In the event where a malware's attempt to create backdoors is successful, attackers can use this opportunity to deny access to IoMT devices [65]. Besides, an attacker can use firmware or software to either destroy medical records, run intrusive or destructive programs, or compromise the reliability, accuracy, and privacy of IoMT devices or systems [5]. In this context, sophisticated malware types that use polymorphic or encryption techniques can cause a denial of services. Thus, in the biomedical domain, preventing malware attacks is of the highest priority as it can inflict serious damage to IoMT systems.

5.3 | Eavesdropping attack

Eavesdropping is one of the most commonly used attack types to collect information from biomedical sensors [66]. Malicious attackers either listens to the message that is being transmitted to detect information (see Figure 3), which is often referred to

as passive eavesdropping [67, 68]. Besides, attackers might also actively collect information by sending multiple friendly queries, which is called active eavesdropping [69]. Attackers also locate the targeted hardware, so that they can intercept it to collect sensitive information. For example, as discussed by [70], the vitals of a patient can get intercepted during transmission. This data can then be used to execute different types of attacks, such as fingerprinting attacks. Besides, with an active eavesdropping attack, eavesdroppers can take advantage of vulnerabilities present in an unsecured network to interrupt communication between two entities, such as sensor nodes or smartphones, without their consent [71, 72]. As a result, the eavesdropper listens to the communication in the hope to obtain critical medical data, which can further be used to masquerade as the claimant.

6 | CURRENT CRYPTOGRAPHIC SOLUTIONS FOR IOMT

Although IoMT systems offer reliable and effective health-care services for doctors and patients, it undoubtedly faces serious security challenges. Due to this, security is considered to be one of the most important concerns in biomedical research, as the patient's privacy-sensitive physiological data can be leaked or misused easily during the medical data lifecycle [20]. Techniques such as access control (see Table 1), identity verification (see Table 2), and data encryption (see Table 3) are some of the most popular approaches that ensure the safety of medical data in IoMT systems. Modern cryptographic techniques have been employed to safeguard the security of wireless communication (see Table 4).

6.1 | Access control

Access control is a technique to avoid unauthorized access to resources by illegal users while determining the adequate authority levels for authorized users [73, 74]. In the case of IoMT systems, access control enables users to restrict access to IoMT devices by defining access levels for each user [5]. It is important to highlight that access control can ensure data confidentiality for IoMT devices [75]. This is apparent in the study of [76], where the authors introduced a lightweight glass-breaking access control algorithm that incorporates two access modes: glass-breaking access and attribute-based access. While glass-breaking access is reserved for emergencies, attribute-based access is utilized to fine-grain access control. According to the authors, their proposed system is secured and displayed highly accurate results. Similar research by [77] proposed a flexible two-fold access control system for an IoMT information storage system. The authors proclaim that their access control system is self-adaptive for both emergency and normal scenarios, and can prevent duplication of medical data through the smart, secure duplication method. Another study by [78] introduced a ciphertext policy that is based on the attribute-based encryption

TABLE 1 Access control techniques

Access control techniques	Features	Advantage	Disadvantage
Lightweight glass-breaking algorithm [76]	Supports two-ways accessing of encrypted medical files: break glass access and attribute-based access.	It can bypass the access protocol of medical files to enable timely access to rescue workers.	Incapable of aborting transactions arbitrarily.
Flexible two-fold access control system [77]	Lightweight, flexible, and fine-grained access control algorithm that can achieve authentication with tailored policies and iterative authorization.	Capable of protecting IT infrastructure from unauthorized access.	Vulnerable against hacking.
Attribute-based encryption algorithm [78]	High data confidentiality, secured access control, high scalability, and improved user accountability	Encrypt and decrypt data based on the attributes of users.	ABE requires data owners to use all the public keys of users to encrypt data.
Slepian Wolf coding algorithm [79]	Supports unlimited parameters.		

TABLE 2 Identity authentication techniques

Identity authentication techniques	Features	Advantage	Disadvantage
Key and authentication agreement protocol[84]	Strong against MiTM attacks	Larger authentication keys.	Depends on the authenticity of private keys.
Session resumption based end-to-end technique [86]	Does not require a public key and certificate-related functionalities. It also requires less ROM and RAM requirements and can provide high-security levels.	End users can communicate without establishing communication from handshake.	Requires good amount of computational power.
Rotating group signature scheme [89]	Can be used in a wide range of application scenarios, including e-business and government portals. It also ensures anonymity and unforgeable tracing verification.	Users can anonymously send message on behalf of the group.	It must follow basic requirement, such as soundness and completeness, unforgeable, anonymity, and traceability.

TABLE 3 Data encryption techniques

Data encryption techniques	Features	advantage	disadvantage
AES-based key distribution scheme [93]	High scalability, high availability, and can perform cyphers as block cyphers or stream cyphers.	It offers efficient scalability and distribution of public keys.	Relatively slow encryption speed.
Secret cipher share algorithm [95]	Data or secret is divided into two parts. It also supports speed and security for server-side aggregation.	Support privacy-preserving data outsourcing.	Have various security limitations.
D2D-Assist data transmission protocol [96]	The higher data rate, coverage extension, low delay, and reliability in communications.	Reduction of demands over cellular networks, higher data rate, quick communication between devices.	No possibility for cellular and D2D simultaneous transmission.

algorithm. In this research, the medical attribute values are hidden in the form of encrypted s-health records (SHRs). With this access control system, the authors successfully addressed the patient's privacy and medical record issues. The research of [79,

80] protected the privacy of patients while eliminating insider attacks by developing a secret data-sharing framework for IoMT devices that uses Slepian Wolf coding algorithm. According to the study, their proposed framework is capable of collaborating

TABLE 4 Summary of cryptographic solutions

Techniques	Advantages	Disadvantages
Access control [74]	Contains varying levels of security. It is also capable of restricting access.	Vulnerable against hacking. It cannot also provide information regarding which users can access which information.
Identity authentication [81]	Spoof-proof, highly secured, and non-transferrable.	High costs, vulnerable to data breaches, false positives, inaccuracy, and bias.
Data encryption [90]	Increased data security, automatic data encoding, and reduced coding errors.	Unable to protect data in transit, requires a tremendous amount of computing resources, and data recovery is complicated.

multiple cloud servers to provide the data of patients to health-care without revealing its content.

6.2 | Identity authentication

Figures Identity authentication is a method of validating the user's identity to prevent unauthorized personnel from gaining access to crucial medical data [81, 82]. On this account, the research of [83] explored a lightweight IoMT storage system. In this system, the researchers employed edge servers to develop a strong identity verification framework that uses data authenticators to verify the patient's identity while protecting sensitive physiology data. Similarly, [84] proposed a key and authentication agreement protocol that make use of the access control mechanism to improve the privacy and data security of doctors and patients. In addition, their lightweight authentication and ownership protocol addresses recent authentication flaws like secure communication but is vulnerable to DoS, desynchronization, and traceability attacks. In [85], and [86], the authors developed an end-to-end scheme using session resumption technique and handshake process for protecting IoMT systems. The authors in [85] proclaim that their proposed scheme can lower the communication latency and communication overhead by 16% and 26%, respectively. On the other hand, in [86], the authors obtained attack detection accuracy of 97%. What makes this scheme more interesting is that it uses 2.2 times less ram and 2.9 times less ROM to run 97% faster than certified-based DTLS schemes. The study of [87] introduced a secured IoMT system based on access control and privacy-aware aggregate authentication mechanism. This system is developed using an anonymous certificate less signature framework to protect a patient's medical records. Another study by [88] introduced a unique update mechanism that can be used to update session keys and authentication keys by using a two-way identity authentication method. This method is efficient in authenticating and identifying the legality of heterogeneous medical sensors. This method uses symmetric encryption in cohesion with the elliptic curve encryption algorithm to eliminate anonymously, and untrusted authentication servers from access medical data. The study of [89], on the other hand, used a rotating group signature scheme that utilizes elliptic curve cryptography (ECC) to ensure patient anonymity. Based on the results, the authors proclaim that their system is capable of resisting attacks while providing several security features.

6.3 | Data encryption

Data encryption is a security technique that translates data into code, or another form so that people having a secret key – decryption key can access the information [90, 91]. This method of security is popular among security practitioners, especially in the biomedical domain, as it ascertains the integrity of medical data [92]. Studies like [93, 94] developed an AES based key distribution and send-receive model scheme to secure the transmission of data in IoMT. Moreover, to allow a privacy-preserving strategy, the authors employed homomorphic encryption that uses a matrix scheme to ensure privacy and an expert detection system to examine the scrambled medical data, automatically. The study authored by [95] proposed a secured data collection framework that improves the security of data transmission and data acquisition. According to the study, the proposed system is designed using two algorithms; one is the secret cipher share algorithm while the other is a lightweight FGPA hardware-based algorithm. In terms of performance, this system has reduced computation time, lower energy consumption high-frequency rate compared to conventional IoT-based healthcare schemes. In the study of [96], the authors introduced a novel D2D-assist data transmission protocol that guarantees the integrity and confidentiality of the transmission of medical data in IoMT. The performance analysis shows that the proposed system is capable of outperforming existing IoMT schemes in terms of communication and computational overhead. Thus, it is evident that various cryptographic solutions are capable of ensuring the safety of IoMT systems.

7 | COUNTER MEASURES

Figures Medical devices are commonly in direct connection with the human body and take care of sensitive information. These devices accumulate crucial health-related information from users and channel it via a wired or wireless communication channel. However, due to advancements in communication technologies, adversaries have started taking advantage of modern solutions to pose the risk of active and passive attacks. To fight against these attacks, researchers have proposed various state-of-the-art countermeasures that are secured and effective enough to prevent cyberattacks (see Table 5). Some of these countermeasures are discussed below.

TABLE 5 Summary of countermeasures

Technique	Overcomes attack	Advantage	Disadvantage
Isolation-based Mechanism [97, 98].	Buffer overflow, MITM, remote code execution.	Capable of verifying the integrity and authenticity of the code present in the trusted zone.	Inefficient against run-time attacks.
Bio-cryptographic key generation [99, 100], [106–116]	MITM, eavesdropping, and tempering	Does not require a key-pre-distribution technique to generate the key.	Vulnerable against attacks that are based on EEG and ECG data.
Attestation-based mechanism [105]	Buffer overflow, and remote code execution.	Performs efficiently in medical device applications.	Vulnerable against data modification attacks.

7.1 | Isolation-based mechanism

This control-flow security mechanism is designed to isolate the resources and assets of a particular application in multiple distinct spaces. To classify the levels of security of resources, the authors in [9] utilize a special bit at the hardware level. To traverse between untrusted and trusted zone, special system calls or entry points at the software level are used. With this method, the authors successfully used CPU to provide APIs and instruction codes to allot secure memory area. Likewise, the study [97–98] – with hardware primitives – provided segregation between different functions. While these techniques depend on the hardware due to the utilization of protected memory protection unit (MPU), it can make use of a microprocessor register to ensure that every isolated function can access the assigned MPU only.

7.2 | Bio-cryptographic key generation

Key generation and agreement is an effective countermeasure against cyberattacks. These techniques use physiological attributes, including IPI, which is unique and random and is perfect for cryptographic [99]. Different practitioners used such key generation schemes to counter cyberattacks. For example, in [100], the authors suggested bio-cryptographic key management protocol for the purpose of protecting the communication of wearable and implantable medical devices. This scheme used physiological parameters, such as an electrocardiogram (ECG), photo plethysmo gram (PPG), and blood pressure from sensors to generate highly secured cryptographic keys. Correspondingly, the authors in [101] proposed a heartbeat based random binary sequence (RBS) protocol to safeguard communication between medical devices. This approach utilized Hamming Distance metric and finite monotonic increasing sequence generation scheme to extract entropic bits from IPI based ECG. The authors proclaim that their approach to bio-cryptographic key generation is efficient and is capable of excerpting up to sixteen random bits.

7.3 | Attestation-based architecture

In order to shut out run-time attacks that impact the control flow and integrity of a device, which is usually caused

by poor programming practices, such as buffer overflows and poor memory management, different countermeasures have been proposed in the literature. For example, in the study [102, 103] Lo-Fat and C-flat architectures have been proposed that determine a value of hash based on path execution that the device takes. This type of architecture works with a verifier and a prover. While the verifier can be considered as a remote computer that manages the flow of the software execution of a device, the prover is the managing software for a low-end device. Similarly, the authors in [104–106] proposed HCFI and HAFIX based schemes that verify that label of every destination node during the flow transfer. In the case of unusual cyberattacks, such as control flow hijacking, these techniques can easily identify it before the cyberattack can jeopardize the security.

8 | GAP ANALYSIS

Table 6 is reprinting the drawbacks of the few of survey papers discussed in this article. There are several drawbacks discussed in the literature review, including incapable aborting transactions, vulnerable against hacking, encryption algorithms use the public keys of users to encrypt data, dependent on the authenticity of private keys, need more computational powers, and slow encryption speed etc.

Using artificial intelligence-based Fuzzy inference systems, machine learning techniques, and data fusion approaches may be used in the future to overcome the problems mentioned above; these disadvantages could be addressed in the future.

9 | CONCLUSION

The state-of-the-art technical innovations with the advent of networked medical devices have changed the dynamics of healthcare operations. As a result, interest in the network security of medical devices has gained significant attention. In addition, it has been identified that with the introduction of new communication technology, such as 5G networks, the healthcare industry will completely revolutionize. We will witness the shift in paradigm in healthcare sector due to the rapid development in communication technology. Modern state-of-the-art healthcare frameworks are incapable of performing telesurgery because of the communication issues. With 5G frameworks,

TABLE 6 Gap analysis of survey papers discussed in literature review

Authors	Technique	Drawbacks
Y. Yang et al., 2017 [76]	Lightweight glass-breaking algorithm	Incapable of aborting transactions arbitrarily
Y. Yang et al., 2019 [77]	Flexible two-fold access control system	Vulnerable against hacking
Y. Zhang, et al., 2018 [78]	Attribute-based encryption algorithm	ABE requires data owners to use all the public keys of users to encrypt data.
S. F. Aghili et al., 2019 [84]	Key and authentication agreement protocol	Depends on the authenticity of private keys.
S. R. Moosavi et al., 2015 [86]	Session resumption based end-to-end technique	Requires good amount of computational power
A. Mehmood et al., 2018 [89]	Signature scheme	basic requirement, such as soundness and completeness, unforgeable, anonymity, and traceability
H. Huang et al., 2017 [93]	AES-based key distribution scheme	Relatively slow encryption speed
F. McKeen et al., 2013 [105]	Attestation-based mechanism	Vulnerable against data modification attacks

ambulance services will be replaced, and wearable devices will be redefined. However, this platform, due to technological advancements, is exposed to different types of security threats and thereby, they might pose a notable risk to the safety and privacy of patients. Consequently, modern security concerns have forced researchers to analyze different vulnerabilities present in medical devices. In addition, since security is an essential element that ensures the reliability of IoMT devices, and for the successful integration of this technology into healthcare systems, there is a need for novel protection schemes that can preserve the integrity and security of IoMT systems. In this regard, the current research highlighted the existing potential threats and attacks that endanger the availability, authorization, authentication, nonrepudiation, integrity, and confidentiality of IoMT devices. Moreover, the study also discussed novel counter security measures, obtained from the literature, against anomalies that threaten IoMT systems. Finally, different approaches and frameworks were presented to ascertain a more robust and enhanced IoMT that can further help in improving the experience and health of patients.

ACKNOWLEDGEMENTS

This work has been supported by the Universiti Kebangsaan Malaysia.

FUNDING

None

CONFLICT OF INTEREST

Authors declare that there is no conflict of Interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Mohammad Kamrul Hasan  <https://orcid.org/0000-0001-5511-0205>

Rashid A. Saeed  <https://orcid.org/0000-0002-9872-081X>

REFERENCES

- Wang, L., Ali, Y., Nazir, S., Niazi, M.: ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods. *IEEE Access* 8, 152316–152332 (2020)
- Nayak, S., Patgiri, R.: A vision on intelligent medical service for emergency on 5G and 6G communication era. *EAI Endorsed Trans. Internet Things* 6(22), 1–13 (2020). <https://doi.org/10.4108/eai.17-8-2020.166293>
- Wu, Y.: Cloud-edge orchestration for the internet-of-things: Architecture and AI-powered data processing. *IEEE Internet Things J.* 8(16), 12792–12805 (2020). <https://doi.org/10.1109/JIOT.2020.3014845>
- Yaqoob, T., Abbas, H., Atiqzaman, M.: Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Commun. Surv. Tutorials* 21(4), 3723–3768 (2019)
- Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., et al.: A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans. Emerging Telecommun. Technol.* e4049 (2020)
- Atamli, A.W., Martin, A.: Threat-based security analysis for the internet of things. In: 2014 International Workshop on Secure Internet of Things, Wroclaw, Poland, pp. 35–43 (2014)
- Haoyu, L., Jianxing, L., Arunkumar, N., Hussein, A.F., Jaber, M.M.: An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. *Future Gener. Comput. Syst.* 98, 69–77 (2019)
- Akhtaruzzaman, M., Hasan, M.K., Kabir, S.R., Abdullah, S.N.H.S., Sadeq, M.J., et al.: HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey. *IEEE Access* 8, 222977–223008 (2020)
- Costan, V., Lebedev, I., Devadas, S.: Sanctum: Minimal hardware extensions for strong software isolation. In: *25th USENIX Security Symposium*, Austin, TX, pp. 857–874 (2016)
- Rani, S., Ahmed, S.H., Talwar, R., Malhotra, J., Song, H.: IoMT: A reliable cross layer protocol for internet of multimedia things. *IEEE IoT J.* 4(3), 832–839 (2017)
- Hassan, R., Qamar, F., Hasan, M.K., Aman, A.H.M., Ahmed, A.S.: Internet of things and its applications: A comprehensive survey. *Symmetry* 12(10), 1–29 (2020)
- Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P., Ni, W.: Anatomy of threats to the internet of things. *IEEE Commun. Surv. Tutorials* 21(2), 1636–1675 (2018)
- Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M.: Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inf.* 14(11), 4724–4734 (2018)
- Islam, S., Abdalla, A.H., Hasan, M.K.: Novel multihoming-based flow mobility scheme for proxy NEMO environment: A numerical approach to analyse handoff performance. *ScienceAsia* 43, 27–34 (2017)

15. Aceto, G., Persico, V., Pescapé, A.: A survey on information and communication technologies for Industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Commun. Surv. Tutorials* 21(4), 3467–3501 (2019)
16. Pustokhina, I.V., Pustokhin, D.A., Gupta, D., Khanna, A., Shankar, K., et al.: An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. *IEEE Access* 8, 107112–107123 (2020)
17. Bhunia, S.S., Gurusamy, M.: Dynamic attack detection and mitigation in IoT using SDN. In: *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne, pp. 1–6 (2017)
18. Cecil, J., Gupta, A., Pirela-Cruz, M., Ramanathan, P.: An IoMT based cyber training framework for orthopedic surgery using Next Generation Internet technologies. *Inf. Med. Unlocked* 12, 128–137 (2018)
19. Joshi, A.M., Jain, P., Mohanty, S.P.: Secure-iGLU: A secure device for non-invasive glucose measurement and automatic insulin delivery in IoMT framework. In: *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Limassol, Cyprus, pp. 440–445 (2020)
20. Yaacoub, J.-P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., et al.: Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* 105, 581–606 (2020)
21. Alsubaie, F., Abuhussein, A., Shiva, S.: Ontology-based security recommendation for the internet of medical things. *IEEE Access* 7, 48948–48960 (2019)
22. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., et al.: Security in IoMT Communications: A Survey. *Sensors* 20(17), 4828 (2020)
23. Alsubaie, F., Abuhussein, A., Shiva, S.: A framework for ranking IoMT solutions based on measuring security and privacy. In: *Proceedings of the Future Technologies Conference*, Vancouver, Canada, pp. 205–224 (2018)
24. Fiadh, J., Mohammed, S.: Security and Vulnerability of Extreme Automation Systems: The IoMT and IoA Case Studies. *IT Prof.* 21(4), 48–55 (2019)
25. Clark, G.W., Doran, M.V. & Andel, T.R.: Cybersecurity issues in robotics. In: *2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA)*, Savannah, GA, USA, pp. 1–5 (2017)
26. Meinert, E., Van Velthoven, M., Brindley, D., Alturkistani, A., Foley, K., et al.: The internet of things in health care in oxford: Protocol for proof-of-concept projects. *JMIR Res. Protoc.* 7(12), e12077 (2018)
27. Sadiku, M.N.O., Eze, K.G., Musa, S.M.: Block chain technology in health-care. *Int. J. Adv. Sci. Res. Eng.* 4(5), 154–159 (2018)
28. Palve, A., Patel, H.: Towards securing real time data in IoMT environment. In: *2018 8th international conference on communication systems and network technologies (CSNT)*, pp. 113–119 (2018)
29. Parmar, A.: Hacker shows off vulnerabilities of wireless insulin pumps. In: *MedCity News*, (2012)
30. Huang, X., Nazir, S.: Evaluating security of Internet of Medical Things using the analytic network process method. *Secur. Commun. Netw.* 2020, 8829595 (2020)
31. Solangi, Z.A., Solangi, Y.A., Chandio, S., bin Hamzah, M.S., Shah, A., et al.: The future of data privacy and security concerns in Internet of Things. In: *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, pp. 1–4 (2018)
32. Alsubaie, F., Abuhussein, A., Shandilya, V., Shiva, S.: IoMT-SAF: Internet of medical things security assessment framework. *Internet Things* 8, 100123 (2019)
33. Hatzivasilis, G., Soulatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., et al.: Review of security and privacy for the Internet of Medical Things (IoMT). In: *2019 15th international conference on distributed computing in sensor systems (DCOSS)*, pp. 457–464 (2019)
34. Alrawais, A., Althothaily, A., Hu, C., Cheng, X.: Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Comput.* 21(2), 34–42 (2017)
35. Guan, Z., Lv, Z., Du, X., Wu, L., Guizani, M.: Achieving data utility-privacy tradeoff in Internet of medical things: A machine learning approach. *Future Gener. Comput. Syst.* 98, 60–68 (2019)
36. Treacy, C., Loane, J., McCaffery, F.: A Developer Driven Framework for Security and Privacy in the Internet of Medical Things. In: *European Conference on Software Process Improvement*, pp. 107–119 (2020)
37. Sadeghi, A.-R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial internet of things. In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6 (2015)
38. Ahlmeyer, M., Chircu, A.M.: Securing the Internet of Things: A review. *Issues Inf. Syst.* 17(4), 21–28 (2016)
39. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., et al.: Security and privacy in the medical internet of things: A review. *Secur. Commun. Netw.* 2018, 5978636 (2018)
40. Sun, Y., Lo, F.P.-W., Lo, B.: Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* 7, 183339–183355 (2019)
41. Sagay, A., Jahankhani, H.: Consumer awareness on security and privacy threat of medical devices. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, pp. 95–116, Springer, Berlin (2020)
42. Li, X., Dai, H.-N., Wang, Q., Imran, M., Li, D., et al.: Securing internet of medical things with friendly-jamming schemes. *Comput. Commun.* 160, 431–442 (2020)
43. Allouzi, M.A., Khan, J.I.: Soter: Trust discovery framework for internet of medical things (IoMT). In: *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 1–9 (2019)
44. Sublett, C.: Cybersecurity of digital diabetes devices. in *Diabetes Digital Health*, pp. 271–283, Elsevier, Amsterdam (2020)
45. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: A review. In: *2012 international conference on computer science and electronics engineering* 3, 648–651 (2012)
46. Banerjee, M., Lee, J., Choo, K.-K.R.: A blockchain future for internet of things security: A position paper. *Digital Commun. Networks* 4(3), 149–160 (2018)
47. Wazid, M., Das, A.K., Rodrigues, J.J.P.C., Shetty, S., Park, Y.: IoMT malware detection approaches: Analysis and research challenges. *IEEE Access* 7, 182459–182476 (2019)
48. Rizk, D., Rizk, R., Hsu, S.: Applied layered-security model to IoMT. In: *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, p. 227 (2019)
49. Chudzikiewicz, J., Furtak, J., Zielinski, Z.: Secure protocol for wireless communication within internet of military things. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, pp. 508–513 (2015)
50. RM, S.P., Maddikunta, P.K.R., Parimala, M., Koppu, S., Gadekallu, T.R., et al.: An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput. Commun.* 160, 139–149 (2020)
51. Manal, R., Fatima, R., Tomader, M.: Authentication for e-health applications in IoT enabled 5G and proposed solution. In: *Proceedings of the 4th International Conference on Smart City Applications*, pp. 1–6 (2019)
52. Melnick, J.: Top 10 most common types of cyber attacks. *Netwrix Blog* (2018). <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>
53. Butun, I., Österberg, P., Song, H.: Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutorials* 22(1), 616–644 (2019)
54. Ibarra, J., Jahankhani, H., Beavers, J.: Biohacking capabilities and threat/attack vectors. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer, Berlin, pp. 117–131 (2020)
55. Mahjabin, T., Xiao, Y., Sun, G., Jiang, W.: A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* 13(12), 1550147717741463 (2017)
56. Singh, S., Rezaii, H.G., Bousquet, J.-F., Craig, J.: Channel access model to predict impact of authentication attack on AIS. In: *OCEANS 2018 MTS/IEEE Charleston*, Charleston, SC, pp. 1–5 (2018)
57. Meng, W., Li, W., Zhu, L.: Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. *IEEE Trans. Eng. Manage.* 67(4), 1377–1386 (2019)

58. Zeadally, S., Adi, E., Baig, Z., Khan, I.A.: Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access* 8, 23817–23837 (2020)
59. Jaramillo, L.E.S.: Malware detection and mitigation techniques: Lessons learned from Mirai DDOS attack. *J. Inf. Syst. Eng. Manage.* 3(3), 19 (2018)
60. Gull, S., Parah, S.A., Muhammad, K.: Reversible data hiding exploiting Huffman encoding with dual images for IoT-based healthcare. *Comput. Commun.* 163, 134–149 (2020)
61. Sun, H.-M., Shen, C.-E., Weng, C.-Y.: A flexible framework for malicious open XML document detection based on APT attacks. In: *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 2005–2006 (2019)
62. Liaqat, S., Akhunzada, A., Shaikh, F.S., Giannetsos, A., Jan, M.A.: SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). *Comput. Commun.* 160, 697–705 (2020)
63. Karmakar, K.K., Varadharajan, V., Tupakula, U., Nepal, S., Thapa, C.: Towards a security enhanced virtualised network infrastructure for Internet of Medical Things (IoMT). In: *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pp. 257–261 (2020)
64. Ahmad, I., Shah, M.A., Khattak, H.A., Ameer, Z., Khan, M., et al.: FIViz: Forensics investigation through visualization for malware in Internet of Things. *Sustainability* 12(18), 7262 (2020)
65. Ullah, F., Naem, H., Jabbar, S., Khalid, S., Latif, M.A., et al.: Cyber security threats detection in internet of things using deep learning approach. *IEEE Access* 7, 124379–124389 (2019)
66. Beavers, J., Pournouri, S.: Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. *Blockchain and Clinical Trial*, pp. 249–267, Springer, Berlin (2019)
67. Kim, M., Hwang, E., Kim, J.-N.: Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas. *Wireless Networks* 23(2), 355–369 (2017)
68. Anh, V.T., Cuong, P.Q., Vinh, P.C.: Context-aware mobility based on π -calculus in Internet of Things: A survey. *Context-Aware Systems and Applications, and Nature of Computation and Communication*, Springer, Berlin, pp. 38–46 (2019)
69. Hamadaqa, E., Adi, W.: Clone-resistant authentication for medical operating environment. In: *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 757–762 (2020)
70. Alsubaie, F., Abuhussein, A., Shiva, S.: Security and privacy in the internet of medical things: Taxonomy and risk assessment. In: *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 112–120 (2017)
71. Yanambaka, V., Mohanty, S., Kougiannos, E., Puthal, D., Rachakonda, L.: PMsec: PUF-based energy-efficient authentication of devices in the Internet of Medical Things (IoMT). In: *2019 IEEE International Symposium on Smart Electronic Systems (ISES) (Formerly iNiS)*, pp. 320–321 (2019)
72. Fadi, A.-T., David, D.B.: Seamless authentication: For IoT-big data technologies in smart industrial application systems. *IEEE Trans. Ind. Inf.* 17(4), 2919–2927 (2020)
73. Wang, X., Wang, L., Li, Y., Gai, K.: Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. *IEEE Access* 6, 47657–47665 (2018)
74. Aftab, M.U., Qin, Z., Hussain, K., Jamali, Z., Son, N.T., et al.: Negative authorization by implementing negative attributes in attribute-based access control model for Internet of Medical Things. In: *2019 15th International Conference on Semantics, Knowledge and Grids (SKG)*, pp. 167–174 (2019)
75. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., et al.: A survey on access control in the age of internet of things. *IEEE IoT J.* 7(6), 4682–4696 (2020)
76. Yang, Y., Liu, X., Deng, R.H.: Lightweight break-glass access control system for healthcare Internet-of-Things. *IEEE Trans. Ind. Inf.* 14(8), 3610–3617 (2017)
77. Yang, Y., Zheng, X., Guo, W., Liu, X., Chang, V.: Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inf. Sci.* 479, 567–592, (2019)
78. Zhang, Y., Zheng, D., Deng, R.H.: Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE IoT J.* 5(3), 2130–2145 (2018)
79. Luo, E., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J., et al.: Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Commun. Mag.* 56(2), 163–168 (2018)
80. Hasan, M.K., Ahmed, M.M., Musa, S.S., Islam, S., Abdullah, S.N.H.S., et al.: An improved dynamic thermal current rating model for PMU-based wide area measurement framework for reliability analysis utilizing sensor cloud system. *IEEE Access* 9, 14446–14458 (2021)
81. Engineer, M., Tusha, R., Shah, A., Adhvaryu, K.: Insight into the importance of fog computing in Internet of Medical Things (IoMT). In: *2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC)*, pp. 1–7 (2019)
82. Hamidi, H.: An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future Gener. Comput. Syst.* 91, 434–449 (2019)
83. Ding, R., Zhong, H., Ma, J., Liu, X., Ning, J.: Lightweight privacy-preserving identity-based verifiable IoT-based health storage system. *IEEE IoT J.* 6(5), 8393–8405 (2019)
84. Aghili, S.F., Mala, H., Shojafar, M., Peris-Lopez, P.: LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* 96, 410–424 (2019)
85. Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.M., Virtanen, S., et al.: End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Gener. Comput. Syst.* 64, 108–124 (2016)
86. Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A.-M., Virtanen, S., et al.: Session resumption-based end-to-end security for healthcare internet-of-things. In: *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 581–588 (2015)
87. Zhang, Y., Deng, R.H., Han, G., Zheng, D.: Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things. *J. Network Comput. Appl.* 123, 89–100 (2018)
88. Cheng, X., Zhang, Z., Chen, F., Zhao, C., Wang, T., et al.: Secure identity authentication of community Medical Internet of Things. *IEEE Access* 7, 115966–115977 (2019)
89. Mehmood, A., Natgunanathan, I., Xiang, Y., Poston, H., Zhang, Y.: Anonymous authentication scheme for smart cloud based healthcare applications. *IEEE Access* 6, 33552–33567 (2018)
90. Wu, L., Zhang, Y., Ma, M., Kumar, N., He, D.: Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things. *Ann. Telecommun.* 74(7), 423–434 (2019)
91. Saračević, M.H., Adamović, S.Z., Mišković, V.A., Elhoseny, M., Maček, N.D., et al.: Data encryption for Internet of Things applications based on Catalan objects and two combinatorial structures. *IEEE Trans. Reliab.* 70(2), 819–830 (2021). <https://doi.org/10.1109/TR.2020.3010973>
92. Jan, M.A., Usman, M., He, X., Rehman, A.U.: SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT. *IEEE IoT J.* 6(2), 1576–1583 (2018)
93. Huang, H., Gong, T., Ye, N., Wang, R., Dou, Y.: Private and secured medical data transmission and analysis for wireless sensing healthcare system. *IEEE Trans. Ind. Inf.* 13(3), 1227–1237 (2017)
94. Hasan, M.K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.H.A., et al.: Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications. *IEEE Access* 9, 47731–47742 (2021)
95. Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M., et al.: Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet Things J.* 6(1), 410–420 (2018)
96. Zhang, A., Wang, L., Ye, X., Lin, X.: Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. *IEEE Trans. Inf. Forensics Secur.* 12(3), 662–675 (2016)
97. Brassler, F., El Mahjoub, B., Sadeghi, A.-R., Wachsmann, C., Koeberl, P.: TyTAN: Tiny trust anchor for tiny devices. In: *Proceedings of the 52nd Annual Design Automation Conference*, pp. 1–6 (2015)
98. Koeberl, P., Schulz, S., Sadeghi, A.-R., Varadharajan, V.: TrustLite: A security architecture for tiny embedded devices. In: *Proceedings of the Ninth European Conference on Computer Systems*, pp. 1–14 (2014)

99. Zhao, H., Xu, R., Shu, M., Hu, J.: Physiological-signal-based key negotiation protocols for body sensor networks: A survey. *Simul. Modell. Pract. Theory* 65), 32–44 (2016)
100. Altop, D.K., Levi, A., Tuzcu, V.: Deriving cryptographic keys from physiological signals. *Pervasive Mob. Comput.* 39, 65–79 (2017)
101. Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S.C., Zhang, Y.-T.: Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans. Biomed. Eng.* 65(12), 2751–2759 (2018)
102. Dessouky, G., Zeitouni, S., Nyman, T., Paverd, A., Davi, L., et al.: Lo-fat: Low-overhead control flow attestation in hardware. In: *Proceedings of the 54th Annual Design Automation Conference 2017*, pp. 1–6 (2017)
103. Abera, T., Asokan, N., Davi, L., Ekberg, J.-E., Nyman, T., et al.: C-FLAT: Control-flow attestation for embedded systems software. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 743–754 (2016)
104. Christoulakis, N., Christou, G., Athanasopoulos, E., Ioannidis, S.: Hcfi: Hardware-enforced control-flow integrity. In: *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, pp. 38–49 (2016)
105. McKeen, F., Alexandrovich, I., Berenzon, A., Rozas, C.V., Shafi, H., et al.: Innovative instructions and software model for isolated execution. *Hasp@isca* 10(1), (2013)
106. Ghazal, T.M., Hasan, M.K., Hassan, R., Islam, S., Norul, S., et al.: security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technol.* 63(1s), 1–9 (2020)
107. Stathiakis, N., Chronaki, C.E., Skipenes, E., Henriksen, E., Charalambus, E., Sykianakis, A., Vrouchos, G., Antonakis, N., Tsiknakis, M., Orphanoudakis, S.: Risk assessment of a cardiology eHealth service in HYGElAnet. *Comput. Cardiol.* 2003, 201–204 (2003)
108. Wang, B., Yao, Y.K., Wang, X.P., Chen, X.Y.: PB-SVM Ensemble: A SVM ensemble algorithm based on SVM. *Appl. Mech. Mater.* 701, 58–62 (2015)
109. Jia, P., Yan, J.: Classification of Wound Infection Data Based On SVM with A Novel Weighted Gaussian RBF Kernel. *Int. J. Hybrid Inf. Technol.* 9(10), 201–210 (2016)
110. Whitman, M.E., Mattord, H.J.: *Management of Information Security*, Course Technology, Boston, MA (2008)
111. McIlwraith, A., *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Gower, Hampshire (2006)
112. Hasan, M.K., Ghazal, T.M., Alkhaifah, A., Abu Bakar, K.A., Omidvar, A., Nafi, N.S., Agbinya, J.I.: Fischer linear discrimination and quadratic discrimination analysis based data mining technique for Internet of Things framework for healthcare. *Front. Public Health* 9, 1354 (2021)
113. Amanlou, S., Hasan, M.K., Bakar, K.A.: Lightweight and secure authentication scheme for IoT networks based on publish-subscribe fog computing model. *Comput. Networks* 199, 108465 (2021)
114. Hasan, M.K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y.A., Nafi, N.S., Ciro Rodriguez, R., Vargas, D.E.: Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things Applications. *Complexity* 2021, 5540296 (2021)
115. Ghazal, T.M., Hasan, M.K., Alshurideh, M.T., Alzoubi, H.M., Ahmad, M., Akbar, S.S., Al Kurdi, B., Akour, I.A.: IoT for smart cities: Machine learning approaches in smart healthcare—A review. *Future Internet* 13(8), 218 (2021)
116. Nurelmadina, N., Hasan, M.K., Memon, I., Saeed, R.A., Zainol Ariffin, K.A., Ali, E.S., Mokhtar, R.A., Islam, S., Hossain, E., Hassan, M.: A systematic review on cognitive radio in low power wide area network for industrial IoT applications. *Sustainability* 13(1), 338 (2021)

How to cite this article: Hasan, M.K., et al.: A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* 16, 421–432 (2022).
<https://doi.org/10.1049/cmu2.12301>