iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54374

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Exploring the Security Challenges in the Cloud enabled IoMT Sector and Promising Solutions Ahead

Md. Afroz[1], Birendra Goswami[2]
Department of Compuetr Sceince & IT YBN University, Ranchi, Jharkhand, India

Abstract: ***The advent of IoT devices has ushered in a new era of connectivity, permeating various facets of contemporary life. This pervasive integration of technology has engendered a future teeming with possibilities, promising manifold benefits for individuals, information management, and operational processes. As individuals find themselves equipped with an increasing amount of leisure time, they are afforded the opportunity to orchestrate comprehensive life cycles that encompass both personal and professional spheres of influence. Notably, the Internet of Medical Things (IoMT) has emerged as a thriving domain, providing hospitals and clinicians with access to sensitive information pertaining to human lives. However, this proliferation of interconnectedness also introduces a concomitant risk—a fertile ground for malicious actors seeking to exploit vulnerabilities inherent in the IoMT infrastructure.***

In light of these circumstances, the establishment of uniform rules and foolproof methodologies becomes imperative. Although numerous organizations have undertaken the task of creating standards, the prevailing system still exhibits openings that expose the product to potential risks. The IoMT network, while boasting several well-established procedures, encounters hindrances to widespread adoption due to a range of issues. One prominent challenge lies in the composition of IoMT networks, which often comprise battery-operated devices characterized by limited processing capacity. This inherent constraint poses a significant hurdle in the path toward achieving widespread adoption and necessitates innovative solutions to address this predicament.

Extensive literature provides an overview of IoT security integrations, and within this context, this article aims to present a concise summary of the IoMT ecosystem. It delves into pertinent aspects such as legislation, challenges surrounding the establishment of standards, and various security measures utilizing cryptographic solutions, PUF-based approaches, blockchain technology, and named data networking (NDN). Through a meticulous analysis of each solution, this article aims to shed light on their respective advantages and downsides, facilitating informed decision-making and fostering a deeper understanding of the intricacies involved. By examining the legislative landscape surrounding IoMT, stakeholders can gain insights into the regulatory frameworks governing the secure deployment of interconnected medical devices. Furthermore, understanding the challenges impeding the establishment of standardized protocols provides valuable perspectives on the current state of IoMT security. Investigating cryptographic solutions, such as encryption algorithms and secure key management, offers a glimpse into how data protection can be fortified. Similarly, exploring PUF-based solutions, which leverage the inherent uniqueness of physical properties, unveils potential avenues to enhance security. The article also delves into the potential of blockchain technology, a decentralized and immutable ledger, and its role in bolstering IoMT security through enhanced data integrity and access control mechanisms. Lastly, the examination of named data networking (NDN) sheds light on its potential to address security concerns by prioritizing content-centric communication and facilitating secure data sharing.

While each security measure presents distinct advantages, such as data confidentiality, integrity, and availability, it is vital to consider the associated trade-offs and potential downsides. By critically evaluating these factors, stakeholders can make informed decisions when implementing IoMT security measures, mitigating risks and ensuring the protection of sensitive medical information. In summary, the increasing accessibility and utilization of IoT devices, particularly within the realm of the IoMT, hold promise for a brighter future. However, it is imperative to address the challenges posed by vulnerabilities in the IoMT infrastructure through the establishment of uniform rules and robust security measures. This article provides a comprehensive overview of the IoMT ecosystem, elucidates the legislative landscape and challenges of standardization, and explores various security measures, allowing stakeholders to make informed decisions in navigating the complex realm of IoMT security.

Keywords: IoMT , Internet of Medical Things; encryption; security and privacy, physical unclonable function

©IJRASET: All Rights are Reserved

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

I. INTRODUCTION

Wireless technology and its associated advancements in wireless communications have become deeply ingrained in our daily lives, owing to the continuous progress in technology. Notably, the Internet of Things (IoT) has emerged as a pivotal driver of the ongoing internet revolution. The IoT facilitates the integration of real-world objects into computer systems, leveraging technological advancements to make this integration increasingly viable [1]. This transformative concept holds immense potential across various sectors, particularly in domains such as home automation and health monitoring [2]. The IoT functions as a network that connects physical objects through wireless networking protocols, enabling the collection and distribution of data using smart healthcare devices and other "Things" [2]. By combining data processing and analytics, the IoT empowers the internet to glean insights and make informed judgments about real-world objects. An alternative term, the "Internet of Objects," is sometimes used to denote this concept. IoT devices encompass a wide range of electrical and electronic devices, each serving diverse purposes and exhibiting varying forms [3]. The applications of IoT span across numerous domains, including home automation, industry, healthcare, energy management, environmental monitoring, and communication systems [3].

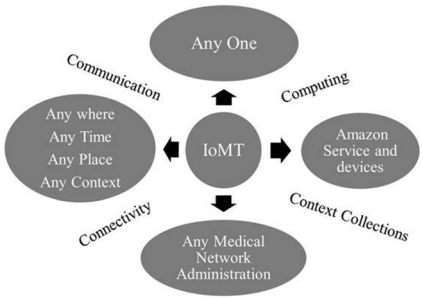


Figure 1. IoMT threats

The increasing interconnectivity of medical devices, facilitated by the IoT, holds significant implications for healthcare. For instance, it promises to enhance the detection and management of chronic illnesses, which is particularly valuable given the global aging population [4]. According to a study by Deloitte, the market is currently inundated with over half a million distinct medical technologies [5]. Within the realm of the IoT, wearable devices and medical/vital monitors are notable examples of Internet of Medical Things (IoMT) devices, designed for use in various settings such as homes, communities, clinics, and healthcare facilities [6]. These devices offer the potential for real-time location tracking, telemedicine services, and other healthcare-related functionalities [6].

The World Health Organization (WHO) defines e-health as the utilization of information and communication technology (ICT) in healthcare settings. Notably, within the field of e-health, there are subfields such as electronic health records (EHR), personal health records (PHR), and mobile health (m-Health), with IoT playing a prominent role in enabling their functionality [7]. Figure 1 illustrates the security concerns associated with IoMT. The IoT environment comprises data-gathering devices, internet connectivity, and software and hardware components responsible for data processing, protection, transmission, and visualization [8]. In practice, sensor data from implantable and wearable devices is transmitted to a cloud server via the internet or a gateway, where it is stored as patient health information (PHI) [6, 9]. Alongside wearables and clinical monitors, the IoMT industry encompasses telemedicine services, other applications, and real-time tracking functionalities [6]. The following sections outline the five key components of the IoMT ecosystem.

II. EASE OF USE

A. The On-Body Section

What is a Body Area Network (BAN)? A BAN is a network medium for transmitting patients' vital signs, which are measured by a wearable or a portable sensor. According to the research of Kocabas et al. [54], biological signals can be used to encrypt communications between medical equipment. Since this is an issue, Poon et al. [55] introduced a low-power bio-identification mechanism that uses an Inter-Pulse Interval (IPI) to encrypt the data exchanged by Body Area Network sensors. Using a secret key of the symmetric key cryptosystem and a physiological signal that agrees on it, Venkatasubramanian et al. [56] were able to communicate BAN sensors. Therefore, there are two methods by which the gathered medical data reaches the controller.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

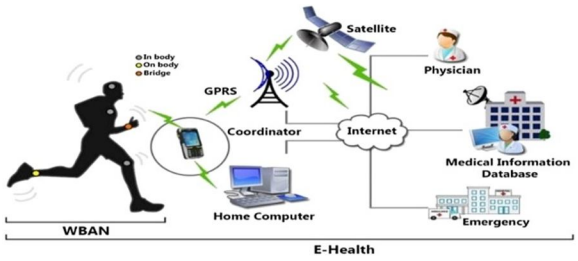


Figure 2. The On-Body Section

B. In Home Section

In this scenario, the home uses sensor data to learn about its residents' health and habits. Mobile devices, display systems, and home robots are all provided to residents, and they are controlled by an autonomous system within the home. [11]. Telehealth services, remote patient monitoring, and personal emergency response systems make up this sector (TVV). The use of such technology paves the way for remote drug management, care for the elderly in the comfort of their own homes, and management of chronic diseases.

1) Seniors and others who rely on them can use PERS's mobility devices (MDs) to stay put. This system combines a wearable gadget or relay unit with a 24/7 medical contact centre to ensure that help is always just a phone call away.

2) RPM: This system uses continuous monitoring of physiological indicators to delay the progression of disease, shorten recovery times, and prevent readmission to the hospital. It includes all sensors and home monitoring systems that can alert users when it's time to take their medications and how much to take.

3) Televisual (TVV): Digital testing and telemedicine are two examples of TVV. It enables people to avoid unnecessary hospitalizations by facilitating the acquisition of necessary medical care, including medicines and suggested treatment regimens.

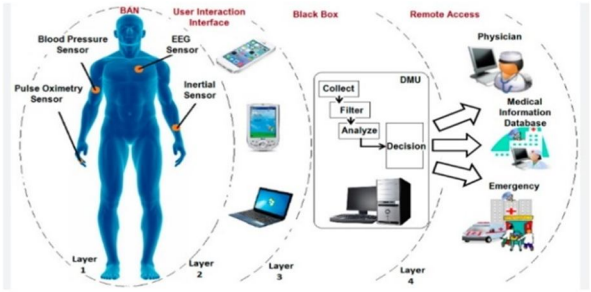


Figure 3. In-Home Section

C. In-Community Section

In the communal part [12], we take local municipal doctors and radio stations into account. The five parts of this section are as follows:

1) *Portability:* While in transportation, patients' vital signs are monitored by this service.

2) *First Responders:* Nurses, and doctors in hospitals' emergency rooms can all benefit from emergency response knowledge.

3) *Kiosks:* These are self-service terminals that may sell goods or offer services like directing users to local healthcare providers.

4) *Point-of-care Technology:* Physicians who provide care in venues other than hospitals, such as mobile clinics and health fairs

5) *logistics:* In the logistics industry, examples of equipment include pressure, temperature, humidity, shock, and tilt sensors for use in the transport of pharmaceuticals..

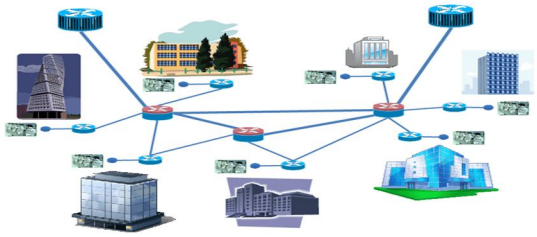


Figure 4. In-Community Section

D. In-Clinic Section

Medical doctors aid in data collection and clinic operations by offering expert advice [6].

1) Medical doctors who work in either an administrative or clinical capacity;
2) Medical doctors with full-time employment in either an administrative or clinical capacity.
3) In this field, qualified individuals can use a product while the service provider is located elsewhere.

E. In- Hospital Section

This category includes IoMT-enabled equipment and solutions for hospital asset, personnel, patient flow, inventory, eenvironmental (temperature, pressure, and humidity), and energy monitoring. In this category [13] you'll find Zoll's wearable defibrillator and Stanley Healthcare's hand-hygiene compliance system.

Eavesdropping, data leak, DoS, physical attacks, cloning, side-channel attacks, remote hijacking, impersonation, password guessing, and man-in-the-middle (MITM) are all hostile threats. Physical attackers must be near the target device. If an attacker takes control of a device, they can clone it to access sensitive data. [16]. As an example of a side-channel assault, timing and power analysis can be used. In an eavesdropping attack, a hacker monitors a network and either steals information or manipulates it by intercepting, erasing, or modifying transmissions between two devices. An attacker can use a man-in-the-middle attack (MITM) to eavesdrop on a conversation between two IoT devices and steal their private information. DoS attacks are launched when a target's resources are blocked [17]. The IoMT network must be protected from intrusion if it is to remain operational.

From the foregoing, it is clear that IoMT is rapidly gaining importance, and a secure setting is necessary for its proper functioning and the protection of sensitive data. The remainder of the text follows the structure of

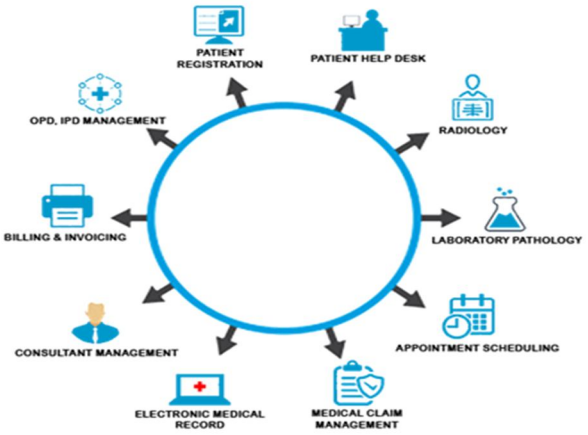


Figure 4. In-Hospital Section.

III. LITERATURE REVIEW

With its close connection to human safety and private data, IoMT is an essential infrastructure. Several types of tests are currently being conducted to determine how best to safeguard the system. This survey study makes an effort to explain the system and recent research achievements in an orderly fashion that facilitates comprehension of the area as a whole. Many writers have surveyed IoMT. Sham-soshoara et al. [18] provided security measures using PUF; Fernández-Caramés et al. [19] demonstrated the difficulty of security measures; Alwarafy et al. [20] introduced intrusion detection using edge computing; Shakeel et al. [21] demonstrated small-scale security systems; Al-Garadi et al. [22], Arora et al. [23], and R. This article discusses security and privacy risks with both centralised and decentralised solutions, as well as implementation issues and constraints. Here's the article's main points*:*

1) IoMT network, device segmentation, and network threats;
2) The significance of the IoMT ecosystem and its role in the modern world;
3) A review of the laws governing medical devices and a list of issues;
4) Security mechanisms that are frequently used for devices with limited resources;
5) Discussion of the advantages and disadvantages of the various proposed security frameworks; these include centralised, decentralised, and NDN.

IV. THE IoMT ECOSYSTEM'S IMPACT ON HEALTHCARE

The use of IoMT is expanding daily. Due to the ecosystem's promising characteristics in the COVID-19 scenario, IoMT adaptability has been promoted higher than in the past. This section will discuss the function of the IoMT system and the expansion of the IoMT market globally.

A. Globat IoMT market

The global IoMT market is expected to grow at a CAGR of 18.5% from 2021 to 2027, reaching USD 284.5 billion by 2027. According to the study, connected MDs constituted up 48% of all MDs in 2020 and 68% by 2025. By 2020, there will be 50,000 pharmaceuticals. IoMT technology might save $300 billion annually in healthcare costs. From 34% in 2020 to 42% in 2025, R&D spending on connected MDs is predicted to rise. Figure 3 The IoMT market is expected to develop at a CAGR of 24.4% to reach USD 254.2 billion by 2026. The smart-wearable-devices category is expected to dominate the market during the projected period, according to All the Research.



Figure 3. Global Internet of Medical Things (IoMT) market from 2016 to 2026 in US dollars [28].

Users don't need to save their data locally since, as said in the cloud data storage system, they store it in the cloud. As a result, the safety, reliability, and accessibility of data files stored on distributed cloud servers are ensured [29]. The global IoMT market will be worth USD 158.1 billion in 2022, up from USD 41 billion in 2017. The industry today spends 34% of its budget on R&D, but it will climb to 42% in five years [30]. By 2040, the elderly population will have doubled, increasing healthcare spending from USD 7.1 trillion in 2015 to USD 8.47 trillion in 2020 [5]. The future medical system will rely totally on IoMT to cut costs, shorten wait times, and improve treatment. Figure shows global IoMT growth to 2030. 4.

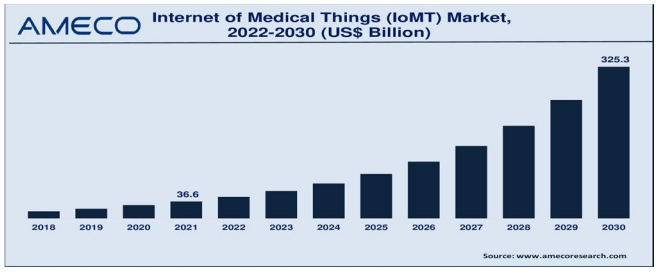


Figure 4. Internet of Medical Things (IoMT) growth forecast for the world

B. Justifications for IoMT Adoption and Implementation

According to the Deloitte report [30], the opportunity for remote patient monitoring, better patient care, and patient happiness are the primary enablers of IoMT adoption, as shown in Figure 5.



Figure 5. The advantages of IoMT systems.

Gus Vlahos, director of healthcare sales for CDW in the Central Region, cites five factors for IoMT acceptability in hospitals. [31].

1) *Boost and Accelerate clinical Workflows:* Conveniently small and portable technologies.These instruments are utilised to carry out crucial tasks like SMS transmission, barcode scanning, and image transmission.
2) *Promotes Closeness:* MD relies on automation and perceptions. Smart drugs and ultrasound machines can provide real-time alerts to hospitals.
3) *Remote Medical Services allow patient-doctor Engagement and Remote Monitoring:* Wi-Fi or Bluetooth-enabled blood pressure cuffs, glucose metres, heart rate monitors, and other gadgets provide patient data to doctors so they may analyse their health and treat appropriately. RPM has enhanced medicine adherence and cut costs in European hospitals.
4) *Proactive Approach to Maintaining Health:* The widespread usage of consumer wearable devices enables the collection and transmission of patient health data to healthcare professionals for necessary assessment and treatment. It offers proactive care as opposed to reactive treatment. New types of sensors are being used in wearable devices like smartwatches and fitness bands to monitor blood oxygen levels, track heart rate, and provide alarms via SMS.
5) *Setting Appropriate Security Measures as a top Priority:* Despite their many advantages, MDs are vulnerable to security risks because of network and device requirements, unfixed default passwords, and occasional (if any) software changes. End-to-end security methods and dependable network monitoring should be given more importance.

C. IoMT's Roles in Healthcare

The IoMT lowers error rates, aids in the accurate diagnosis of diseases, saves operational costs for healthcare organisations, and enables remote patient-doctor communication. IoMT has resulted in USD 2.5 million in savings in a year, a 90% reduction in patient admission time, a 33% reduction in cardiac-resynchronization treatment stay length, a 37% reduction in procedure cancellations due to better patient planning and scheduling, and a 43% reduction in staff overtime. It's been employed with other measures to stop the transmission of COVID-19, which is crucial in the present outbreak.

It creates a barrier for the protection of front-line workers, boosts productivity, lessens the toll the disease takes on people's lives, and finally lowers the mortality rate. Because of IoT's scalability, a sizeable fraction of patients can be monitored remotely from their homes or hospitals without requiring an in-person visit. According to All the Research, the global COVID-19 epidemic is hastening the adoption of IoMT and is essential to the development of the technology. WSN, Bluetooth, ZigBee, WiFi, NB-IoT, LTE, 4G, and 5G, as well as big data, AI, and cloud computing are creating a powerful health-tech ecosystem. [32].

V. THE NEED FOR INTEGRITY AND SAFETY IN THE IOMT SYSTEM

The data that is handled by the environment has grown more susceptible to attack as a result of the broad adoption of IoMT. At the event that an attacker with malicious intent gains access to the environment, not only will sensitive user data be put at risk, but also the life of the patient may be in jeopardy in some circumstances. Through study and the cooperation of the community, a great number of these vulnerabilities have been uncovered. This section will discuss some of the vulnerabilities that are prevalent in IoMT environments, as well as the laws that are in place to protect against those weaknesses.

A. Security Incidents at the IoMT

Safeguarding patients' confidentiality and privacy (SNP) is crucial to building a reliable healthcare system that delivers excellent care. When compared to other systems, the healthcare sector is unique since people' lives and health depend on it. Computing-system security safeguards hardware, software, and data, also known as the CIA trinity. The three tenets of information security are (1) secrecy; (2) prevention of illegal access to data and maintenance of trustworthiness in protecting data resources; and (3) availability. Criminals are always coming up with new ways to break into corporate networks in order to steal sensitive information, alter existing files, or blackmail the company's employees. Many breaches in security have been experienced by IoMT. About 115 cyberattacks were reported throughout January 2018. Over 2.9 million Health South-East RHF subscribers were affected by the incident. The WannaCry ransomware assault on England's NHS was one of the most serious and devastating medical breaches, resulting in 19,000 cancelled appointments and GBP 92 million in mitigation and recovery costs. [33].

There has been at least one security compromise at 90% of healthcare companies using IoMT. Another analysis indicated that over 370 businesses using the IoMT (35% of all businesses) experienced at least one cybersecurity compromise in 2016. In fact, in 2017, 45 percent of all ransomware assaults were directed towards IoMT. MEDJACK 2 demonstrated that ransomware attacks could be successfully instantiated in IoMT settings, leading to data theft. The greatest ransomware assault ever recorded in 2017 hit over 200 thousand devices throughout the world [34].

CyberMDX, a healthcare cybersecurity vendor, discovered an authentication vulnerability in multiple GE Healthcare machines in December 2020, The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued an advisory to all hospitals and medical delivery organisations due to the danger to protected health information. 9.8 is quite severe. MedTronic MyCareLink (MCL) MDs may interfere with clinical data, according to a new alert. All versions of the MCL Smart Model 25000 Patient Reader were discovered to be susceptible. Forescout Research Labs uncovered 33 weaknesses in four open-source TCP/IP stacks that might impact 150 enterprises and millions of MDs. The AMNESIA:33 vulnerabilities affect DNS, IPv6, and TCP [35]. Indiana hospital spent $50,000 in 2018 to restore its data. MD manufacturers who responded yes to Irdeto 2019's question about cyberattacks on their products in the year preceding to the survey [36] are displayed in Figure 6.

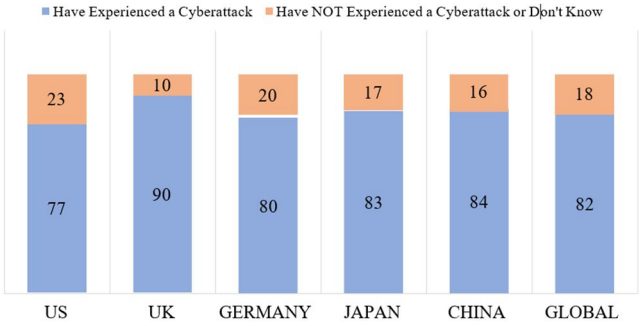


Figure 6. 2019 Irdeto survey.

B. Guidelines for Cybersecurity in the IoMT

Governing agencies are revising pre-market cybersecurity rules for MDs to mitigate user and patient safety hazards. The Food and Drug Administration (FDA), which regulates the MD market, closely monitors MD security issues to safeguard patient safety. FDA provided Premarket Submissions for Cybersecurity Management guidelines in October 2014. These standards prompted recommendations for increased security management and risk reduction to protect device operations. To prevent cybersecurity problems, MD makers must follow the below design and development criteria. As part of software validation and risk assessment, they were instructed to establish a cybersecurity vulnerability and management methodology. The 2016 draught recommendation on postmarket management [37] suggested implementing a cybersecurity risk-management programme during both premarket and postmarket lifecycle stages. In 2018, a suggested new pre-market guidance category for linked Tier 1 and Tier 2 MDs was presented for public feedback.

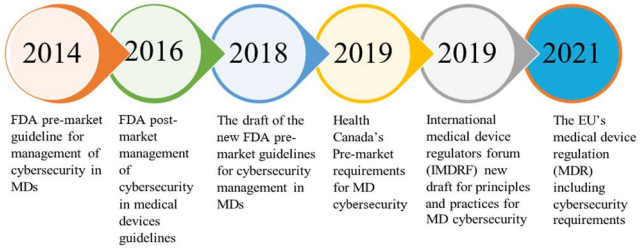


Figure 7. Advances in the cybersecurity regulations for medical devices.

VI. SAFEGUARDING SYSTEMS

There are primarily two kinds of security measures used in each IoT environment: software-based and hardware-based. When it comes to safeguarding computer systems, many have turned to software-based security solutions, which employ mathematical techniques. While current mathematical methods take time to solve, with the advent of quantum computers, key extraction will be much faster. Hardware-based security solutions use encryption algorithms like KPI, AES, and ECC. The former involves shared-key configurations with the server or other devices. Despite its advantages in terms of low computing complexity and great efficiency, it is unrealistic because it shares important characteristics in the case of a large number of devices. Asymmetric protocols, on the other hand, don't need any shared-parameter keys in advance. Both the public and private keys are used. Here, privacy is ensured by using secret keys [38]. In such a device-dense setting, the challenges in enabling secure communication for IoT are device authentication and key exchange.

These MDs also have low requirements for processing speed, energy, and storage space. To ensure safety, many scientists are working on developing an authentication mechanism. When compared to other authentication systems (AS), PUF is notable for its low power consumption and speed in determining whether or not a user is legitimate. When utilized for authentication in IoMT, PUF's digital fingerprint provides a physically defined security primitive. A PUF is a tangible thing that provides a distinct response to a specific question or issue. As a result of the inherent physical diversity of integrated circuits, it is possible to use this as a challenge-response mechanism in security contexts [39]. Because of the unpredictable and uncontrollable side effects of the integrated circuit manufacturing process, PUF is one-of-a-kind and cannot be replicated. In order to authenticate users, PUFs must be able to produce a unique challenge-response pair (CPR) when requested.

VII. PROTECTION MEASURES FOR THE INTERNET OF THINGS

This section will review the available literature on the topic of IoMT network security solutions. All of the plans are laid out in the clearest way possible.

Chiou et al. [40] created an authentication technique to protect IoMT in 2016. As Deebak et al. [41] showed, Chiou et alsolution .'s lacks comprehensive protection to resist security attacks and does not conceal patient identities. Both Ref. [40] and [41] used secret keys to authenticate users, while Ref. [40] communicated the secret key over a public channel whereas Ref. [41] encrypted it with other parameters. Despite Deebak et alimprovements .'s to authentication, Chiou et al.

According to Park et al. [42], Xu et al. [43]'s system is prone to impersonation, stolen senor node, and leaking verification table attacks, and it does not ensure privacy, invisibility, or trustworthiness for its users. Since Xu et al[43] stored authentication parameters as plaintext, a hacked sensor node can be used to launch an impersonation attack by an attacker who signs in to use the stolen parameters to produce a nonce. Park et al. [42] handled these difficulties by not storing client authentication parameters or sensitive data on the server. During registration, when an intermediate node is assigned for sensor-to-server connection, a single point of failure can occur. By combining XOR and hash algorithms, it produces a lightweight authentication system that can build a session key.

Using chaotic maps, Chen et al. [44] established group-oriented time-bound authenticated key agreement. Chaotic maps [45] have a large parameter space, uniform data distribution, and semigroup structure. Permitted entities can only utilise a group key for a limited time before it expires and a new key must be produced. The server transmits an authentication window and available time to service providers and user groups. If the application provider gets a matching token before the time limit, authentication will succeed. If one member of a group is approved first, the remainder can use the authentication token. It's unclear how a group's shared authentication token will be distributed.

Li et al. [46] recommended Hash and XOR as lightweight methods. Six steps employ open channels. Before deployment, a sensor and trusted gateway share a secure key. User and sensor node can join gateway registration with this private key. With Gateway's help, the sensor and user negotiate a session key to encrypt sensor data.

A. Attribute Based

Zhang et al. [47] presented an ABE authentication mechanism. Both centralised and attribute authorities are needed. To authenticate with the cloud, users must send a signed secret key and transformation key to the cloud user assistant. ABE-based systems have problems.

No one can tell who is using a secret key or catch a fraudster who distributes keys without permission. Second, more attributes increase ciphertext size. Decryption takes longer [48]. ABE is too expensive for lightweight devices to decrypt [49].

Liu et al. [50] suggest connecting wearables to a hospital-based edge computing server. Client and server produce pseudo-numbers and compute data attributes with numbers and secret keys to authenticate. In this setup, we partition the secret key into n pieces for computations and transmission. IoT devices shouldn't have to undertake a lot of data processing and storage. Similar to Kumar et al., not all attacks (DoS, Reply, etc.) were countered. Hwang et al. [48] proposed ciphertext-policy attribute-based authentication to tackle this problem (CP-ABE).

This protocol relies on a combination of trusted authority and attribute authority to determine the first key issuer. When there are a fixed number of characteristics, the decryption time is independent of the number of attributes because the ciphertext size is constant. Identity verification in the suggested approach, however, requires a large amount of computing. It also has the problem of confidential information being leaked by the recipient of the delegated key.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Analyzing Heart Rate Via Electrocardiogram

By applying singular value decomposition to de-noise electrocardiogram (ECG) signals, Huang et al. [51] created an ECG-based authentication scheme (SVD). The background noise will be decreased using motion detection and standard feature templates. By employing weighted online SVD, we were able to generate a de-noised signal in the case of mild activity. The angular distance for walking and running is difficult to obtain, and so are many other activities in a wide variety of workouts and situations. The authors assume that intruders cannot obtain ECG templates from patients in their study. There is insufficient protection for user identities, and the computation time is excessive.

C. MAC-Based System Requirement

Data from medical devices (MDs) is collected by a gateway and stored in the cloud using a MAC protocol, as described by Xu et al. [9]. If data is shared in advance with a reliable party, they can use that information to encrypt it. MAC is an authentication system that can be used to check the origin and safeguard the data. Lack of security in data transfer between IoT devices and the gateway. Additionally, a secure channel is needed to transmit the computed key to the IoT gateway.

The suggested authentication methodology for smart cards and MDs uses public-key cryptography. It verifies user IDs using MAC addresses. The server will supply a hash function with a missing k-bit, and the reader device must calculate and identify it. The proposed protocol lacks user privacy.

Hahn et al. [49] devised a mechanism in which a key server creates both a verification key and a commitment key. With these data, users may evaluate their dedication and spread the word. Using the verification key and commitment key, a doctor can verify the commitment key.

D. ML-Based System Requirement

A privacy-protecting outsourced support vector machine Wang et al. [52] recommended using eight privacy-preserving outsourced computation techniques. The proposed protocol outsources integer and floating-point computations for efficiency and correctness. For secure and private processing, the floating-point number was normalised to 2E fixed-point precision. A trusted third party distributes a public-private key pair to all users and then sits idle. Cloud service provider and server have private keys.

VIII. BLOCK CHAIN BASED

Abdellatif et al. [53] propose a holistic framework for Abdellatif et al. [53] propose integrating edge computing and blockchain to process medical data. Initially, an automatic patient-monitoring strategy was devised, and this blockchain system has three channels for separating urgent data. To provide the shortest feasible latency, urgent data was given top priority, and it will function with a less-restricted blockchain by supporting quick response. This work focuses on defining priorities and feature extraction.

Healthchain is a proof-of-work blockchain technology that encrypts health data for access control. Healthchain has Userchain and Docchain. Symmetric AES encryption encrypts IoT data. Docchain's accounting nodes, which operate as miners, add doctor nodes' data to the blockchain. If the IoT key or diagnosis key is compromised, the user can send a fresh key transaction. SHA-256 is utilised for hashing, and 1024-bit RSA for asymmetric encryption and signing. This work provides conditional security because both patients' and doctors' private keys are secure and adversaries' computer power is restricted. Identifying fraudulent transactions and nodes requires a third-party audit.

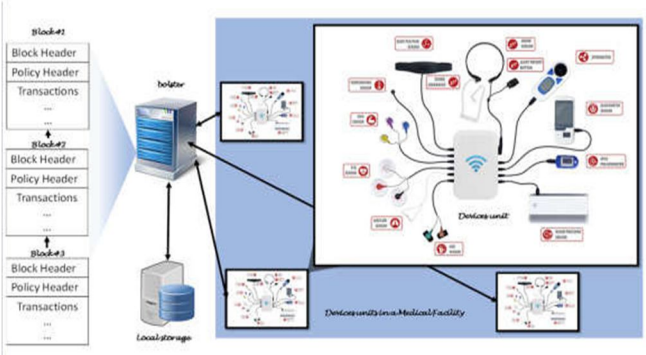


Fig [57] : Introduction to the structure of the blockchain-based IoMT system

IX. CONCLUSION

As the proliferation of internet-connected real-world items continues to expand, so does the concern regarding potential security vulnerabilities within IoT systems. Safeguarding these systems necessitates ongoing efforts by researchers and industry experts to identify and rectify any weaknesses that may be exploited. Various approaches are currently being explored and developed as potential solutions. It is imperative to establish a universal standard upheld by manufacturers to ensure the security and consistency of the IoT ecosystem. Regulatory organizations, such as the Food and Drug Administration (FDA) and the European Union (EU), are actively engaged in developing new regulations and revising existing ones to address these gaps. Compliance with these regulations is a prerequisite for manufacturers seeking to bring their products to market. This study aims to present a comprehensive examination of the IoT ecosystem, its roles, and the associated risks.

The research conducted in this study encompasses an extensive exploration of existing IoT security techniques aimed at enhancing security and privacy. Authentication technologies such as Attribute-Based Encryption (ABE), Elliptic Curve Cryptography (ECC), Message Authentication Codes (MAC), Machine Learning (ML), Physical Unclonable Functions (PUF), and Blockchain have been compared to determine their efficacy. The implementation described in this study utilizes Named Data Networking (NDN) technology, which is undergoing continuous refinement. Crucial barriers to the integration of IoMT systems, including scalability, memory requirements, computing resources, communication overhead, energy efficiency, and security considerations, are given due consideration.

Future research endeavors will delve into the post-quantum and post-5G possibilities of IoMT, exploring potential advancements and implications in these areas. Additionally, the study will address prevailing security issues, such as the vulnerability identified in June 2022 that allows for remote exploitation of cryptographic keys in CPUs manufactured by Intel, AMD, and other vendors. Furthermore, an investigation into the causes of these flaws and potential remedies will be undertaken, aiming to fortify the security posture of IoMT systems.

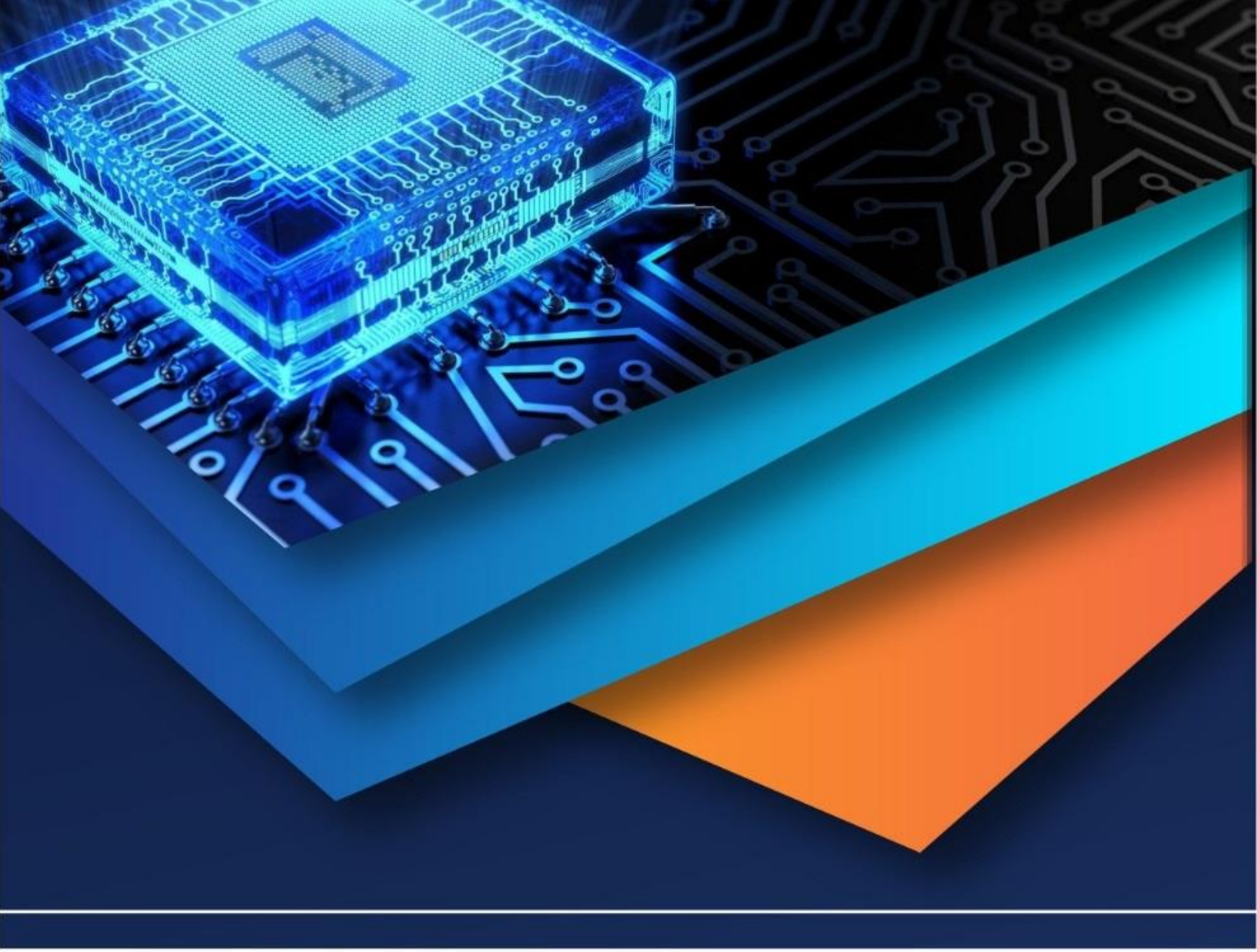
In summary, securing IoT systems against potential vulnerabilities is a paramount concern as the number of internet-connected devices grows exponentially. The establishment of a universal standard upheld by manufacturers and the enactment of robust regulatory frameworks play pivotal roles in ensuring the security and consistency of the IoT ecosystem. Through a comprehensive analysis of existing IoT security techniques and exploration of emerging technologies, this study contributes to the ongoing efforts to enhance the security and privacy of IoMT systems. Future research endeavors will expand upon these findings, delving into advanced post-quantum and post-5G possibilities, addressing prevailing security issues, and exploring potential causes and remedies for identified flaws.

REFERENCES

[1] Tran-Dang, H.; Krommenacker, N.; Charpentier, P.; Kim, D.S. Toward the Internet of Things for Physical Internet: Perspectives and Challenges. IEEE Internet Things J. 2020, 7, 4711–4736
[2] Wazid, M.; Singh, J.; Das, A.K.; Shetty, S.; Khan, M.K.; Rodrigues, J.J.P.C. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. IEEE Access 2022, 10, 57990–58004
[3] Amin, F.; Majeed, A.; Mateen, A.; Abbasi, R.; Hwang, S.O. A Systematic Survey on the Recent Advancements in the Social Internet of Things. IEEE Access 2022, 10, 63867–63884
[4] Sadhu, P.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. NAHAP: PUF-Based Three Factor Authentication System for Internet of Medical Things. IEEE Consum. Electron. Mag. 2022
[5] Internet of Medical Things Market. Available online: https://www2.deloitte.com/ie/en/pages/life-sciences-and-healthcare/ articles/internet-of-medical-things.html
[6] . Internet of Medical Things Revolutionizing Healthcare. Available online: https://aabme.asme.org/posts/internet-of-medical- things-revolutionizing-healthcare/
[7] Alamri, B.; Crowley, K.; Richardson, I. Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review. IEEE Access 2022, 10, 59612–59629
[8] Aledhari, M.; Razzak, R.; Qolomany, B.; Al-Fuqaha, A.; Saeed, F. Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions. IEEE Access 2022, 10, 31306–31339
[9] Xu, C.; Wang, N.; Zhu, L.; Sharif, K.; Zhang, C. Achieving Searchable and Privacy-preserving Data Sharing for Cloud-assisted E-healthcare System. IEEE Internet Things J. 2019, 6, 8345–8356
[10] Hernandez, S.; Raison, M.; Torres, A.; Gaudet, G.; Achiche, S. From on-body Sensors to in-body Data for Health Monitoring and Medical Robotics: A Survey. In Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS), Montreal, QC, Canada, 15–19 September 2014; pp. 1–5
[11] Noguchi, H.; Mori, T.; Sato, T. Framework for Search Application based on Time Segment of Sensor Data in Home Environment. In Proceedings of the Seventh International Conference on Networked Sensing Systems (INSS), Kassel, Germany, 15–18 June 2010; pp. 261–264
[12] Internet of Medical Things (IoMT) Market By Component, Platform, Connectivity Devices, Application and Is Expected to Reach USD 1,84,592.31 Million by 2028. Available online: https://www.marketwatch.com/press-release/internet-of-medical-things- iomt-market-by-component-platform-connectivity-devices-application-and-is-expected-to-reach-usd-18459231-million-by-20 28-2022-04-26
[13] What Is the Internet of Medical Things (IoMT)? Available online: https://mobius.md/2019/03/06/what-is-the-iomt/ (accessed on 22 June 2022)

[14] Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. IEEE Internet Things J. 2021, 8, 15694–15703
[15] Saheed, Y.K.; Arowolo, M.O. Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. IEEE Access 2021, 9, 161546–161554
[16] Hameed, K.; Garg, S.; Amin, M.B.; Kang, B.; Khan, A. A Context-aware Information-based Clone Node Attack Detection Scheme in Internet of Things. J. Netw. Comput. Appl. 2022, 197, 103271
[17] Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl. 2020, 149, 102481
[18] Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A Survey on Physical Unclonable Function (PUF)-based Security Solutions for Internet of Things. Comput. Netw. 2020, 183, 107593
[19] Fernández-Caramés, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet Things J. 2020, 7, 6457–6480
[20] Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in Edge- Computing-Assisted Internet of Things. IEEE Internet Things J. 2021, 8, 4004–4022
[21] Shakeel, T.; Habib, S.; Boulila, W.; Koubaa, A.; Javed, A.R.; Rizwan, M.; Gadekallu, T.R.; Sufiyan, M. A Survey on COVID-19 Impact in the Healthcare Domain: Worldwide Market Implementation, Applications, Security and Privacy Issues, Challenges and Future Prospects. Complex Intell. Syst. 2022, 1–32
[22] Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Commun. Surv. Tutor. 2020, 22, 1646–1685
[23] Arora, P.; Kaur, B.; Teixeira, M.A. Machine Learning-Based Security Solutions for Healthcare: An Overview. Emerg. Technol. Comput. Commun. Smart Cities 2022, 649–659
[24] Rbah, Y.; Mahfoudi, M.; Balboul, Y.; Fattah, M.; Mazer, S.; Elbekkali, M.; Bernoussi, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey. In Proceedings of the 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 3–4 March 2022; pp. 1–9
[25] Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. IEEE Access 2021, 9, 54478–54497
[26] Khor, J.H.; Sidorov, M.; Woon, P.Y. Public Blockchains for Resource-Constrained IoT Devices—A State-of-the-Art Survey. IEEE Internet Things J. 2021, 8, 11960–11982
[27] Awad, A.; Fouda, M.M.; Khashaba, M.M.; Mohamed, E.R.; Hosny, K.M. Utilization of mobile edge computing on the Internet of Medical Things: A survey. ICT Express 2022
[28] Global Internet of Medical Things (IoMT) Market. Available online: https://www.alltheresearch.com/report/166/internet-ofmedical-things-market
[29] Afroz, M., ; Goswami, B. (2022). "A vulnerability to storage security for cloud computing". Lecture Notes in Networks and Systems. In-press. https://doi.org/Congress on Intelligent Systems
[30] How Connected Medical Devices Are Transforming Health Care. Available online: https://www2.deloitte.com/global/en/
[31] 5 Reasons IoMT Devices Make Sense for Healthcare Organizations. Available online: https://healthtechmagazine.net/article/2020/04/5-reasons-iomt-devices-make-sense-healthcare-organizations/
[32] Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT Amid COVID-19 Pandemic: Application, Architecture, Technology, and Security. J. Netw. Comput. Appl. 2020, 174, 102886
[33] Jahankhani, H.; Ibarra, J. Digital Forensic Investigation for the Internet of Medical Things (IoMT). Forensic Leg. Investig. Sci. 2019,5, 29
[34] Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework.Internet Things 2019, 8, 100123.
[35] Medical Device Security. Available online: https://healthitsecurity.com/tag/medical-device-security/
[36] Medical Device Cybersecurity in the Age of IoMT. Available online: https://www.medtechintelligence.com/column/medicaldevice-cybersecurity-in-the-age-of-iomt/
[37] Wu, L.; Du, X.; Guizani, M.; Mohamed, A. Access Control Schemes for Implantable Medical Devices: A Survey. IEEE Internet Things J. 2017, 4, 1272–1283
[38] Li, S.; Zhang, T.; Yu, B.; He, K. A Provably Secure and Practical PUF-based End-to-End Mutual Authentication and Key Exchange Protocol for IoT. IEEE Sensors J. 2020, 21, 5487–5501
[39] Aman, M.N.; Javaid, U.; Sikdar, B. A Privacy-preserving and Scalable Authentication Protocol for the Internet of Vehicles. IEEE Internet Things J. 2020, 8, 1123–1139
[40] Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment. J. Med. Syst. 2016, 40, 10
[41] Deebak, B.D.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems using Internet of Medical Things. IEEE J. Sel. Areas Commun. 2020, 39, 346–360
[42] Park, K.; Noh, S.; Lee, H.; Das, A.K.; Kim, M.; Park, Y.; Wazid, M. LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification Table in Medical Internet of Things. IEEE Access 2020, 8, 119387–119404
[43] Xu, Z.; Xu, C.; Liang, W.; Xu, J.; Chen, H. A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things. IEEE Access 2019, 7, 53922–53931
[44] Chen, M.; Lee, T.F. Anonymous Group-oriented Time-bound Key Agreement for Internet of Medical Things in Telemonitoring Using Chaotic-maps. IEEE Internet Things J. 2021, 8, 13939–13949
[45] Dharminder, D.; Gupta, P. Security Analysis and Application of Chebyshev Chaotic Map in the Authentication Protocols. Int. J. Comput. Appl. 2019, 43, 1095–1103
[46] Li, J.; Su, Z.; Guo, D.; Choo, K.K.R.; Ji, Y. PSL-MAAKA: Provably-Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. IEEE Internet Things J. 2021, 8, 13183–13195

[47] Zhang, L.; Ye, Y.; Mu, Y. Multiauthority Access Control With Anonymous Authentication for Personal Health Record. IEEE Internet Things J. 2020, 8, 156–167
[48] Hwang, Y.W.; Lee, I.Y. A Study on CP-ABE-Based Medical Data Sharing System with Key Abuse Prevention and Verifiable Outsourcing in the IoMT Environment. Sensors 2020, 20, 4934
[49] Hahn, C.; Kwon, H.; Hur, J. Trustworthy Delegation Toward Securing Mobile Healthcare Cyber-physical Systems. IEEE Internet Things J. 2018, 6, 6301–6309
[50] Liu, H.; Yao, X.; Yang, T.; Ning, H. Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-based Smart Health. IEEE Internet Things J. 2018, 6, 1352–1362
[51] Huang, P.; Guo, L.; Li, M.; Fang, Y. Practical Privacy-preserving ECG-based Authentication for IoT-based Healthcare. IEEE Internet Things J. 2019, 6, 9200–9210
[52] Wang, J.; Wu, L.; Wang, H.; Choo, K.K.R.; He, D. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. IEEE Internet Things J. 2020, 8, 458–473
[53] Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; O'Connor, M.D.; Laughton, J. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet Things J. 2021, 8, 15762–15775
[54] Ovunc Kocabas, Tolga Soyata, and Mehmet K Aktas. Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics, 13(3):401416, 2016
[55] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine, 44(4):73–81, 2006
[56] Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S Gupta. Pska: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine, 14(1):60–68, 2010
[57] Seliem, Mohamed & Elgazzar, Khalid. (2019). BIoMT: Blockchain for the Internet of Medical Things. 10.1109/BlackSeaCom.2019.8812784.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)