INVESTIGATING THE IMPORTANCE OF ETHICS AND SECURITY ON INTERNET OF MEDICAL THINGS (IoMT)

Asaad Ali Karam

Associate Professor, University of Duhok, Iraq

asaad.ali@uod.ac

ABSTRACT

Numerous opportunities are emerging due to the Internet of Things' (IoT) rapid development, which has the potential to significantly improve human quality of life in many areas. The healthcare industry is the main place where IoT can enhance our quality of lives. Security and privacy concerns, however, take center stage in electronic health (eHealth) systems, and the incorporation of IoT makes them increasingly difficult to address. Due to the numerous stakeholders in its broader ecosystem, the majority of IoMT which raises security concerns. The IoT-based healthcare system has various security features. This search provides an Identity-Based Cryptography cornerstone management technique that uses collaborative authentication and a secret passcode to protect transformation of data between any IoT health device and any other entity from a different company or domain (IBC).

***Keywords*:** Ethics, Security, Internet of Medical Things (IoMT).

1. INTRODUCTION

The delivery of health care services has changed as a result of the IT and medical industries' convergence, or eHealth. E-Health provides a fresh method of using health resources, such as data, cash, and pharmaceuticals. It assists all concerned parties in making better use of those resources [1]. According to the McKinsey Global Institute, IoT-based hospitals applications will have the greatest economic impact compared to other IoT apps by 2025, growing the global economy by between 1.1 and 2.5 trillion dollars annually [2]. It demonstrates that IoT hospitals has a highly promising result. In terms of the advantages it will

bring to individuals, technology, and the economy [3]. Despite all the positive information regarding IoT-based healthcare solutions, security and privacy remain major issues [4], [5].

IoT-based hospital systems face numerous security plus privacy challenges, including hackers attack, security of the communication channel and ecosystem (such as multi-factor authentication, key management, and cryptographic support), and stealing attempts of the stored information, etc [6]. Yet, the Health Insurance Portability and Accountability must be complied with any IoT device that transmits patient health information (HIPAA). The limited power, processing, and memory capabilities of IoT devices also indicate that the security mechanism must make effective use of those resources [7]. Additionally, the design of IoT-based health care systems generally comprises a number of stakeholders that are members of several organizations with varying security domains and policies, which makes the security work more challenging [8].

In light of the above-described conditions, it is crucial to offer serious management that facilitates multiple methods and safe data transfer among devices within the IoT-based health care system [9].

This research provides an IBC-based security system that help all previously mentioned functionalities. The Identity Based encryption topic was selected considering it is essentially an asymmetric key scheme, which is simpler to distribute keys for [10]. Additionally, unlike other asymmetric key schemes, such as Elliptic Curve Cryptography, it does not need a certificate for practical key distribution. The method, which was created using a variation of Identity Based Encryption that fixes the key escrow issue in the Identity Based cryptography, offers mutual authentication and agreement for secure connection entities across various companies or domains[11].

2. LITERATURE REVIEW

2.1 Safety Challenges and Solutions

The security issues with the IoT-based healthcare system are discussed in this section. There are two primary kinds of challenges: those relating to the inherent nature of the IoT, which has an influence on security solutions; and those relating to IoT system security, particularly in the domain of health care [12]. Additionally, a few potential answers to the problems discussed are offered based on some related publications. Low-speed CPUs are built into Internet of Things health devices [13]. Such gadgets have a slow central processing unit

(CPU) that isn't particularly powerful. Additionally, computationally intensive operations cannot be carried out by these devices [14]. They only serve as a sensor or actuator, in other words. Therefore, it might be difficult to identify a security solution that enhances security performance while minimizing resource usage [15]. However, as the number of IoT devices has increased steadily, more and more devices are joining the world data network. Therefore, creating a highly scalable security system without sacrificing security standards is a different difficult task. Medical records include extremely confidential information regarding a patient's data and health statues that needs to be kept safe and secret from any hackers [16], [17].

In order to comply with HIPAA, hospitals and other healthcare organizations must securely communicate patients' sensitive information [18]. If the automated data gathering isn't validated and handled appropriately, security breaches and privacy violations are quite likely due to the widespread and omnipresent nature of IoT [19]. Without real-time monitoring, patients' private and sensitive medical information may be altered, misused, or compromised. This poses a grave threat to infrastructure in addition to having a devastating effect on people's lives. Apps and wearable technology might be taken over by malicious users, who could then access users' sensitive information and pose grave security and health threats [20]. In order to comply with HIPAA, hospitals and other healthcare organizations must securely communicate patients' sensitive information. If the automated data gathering isn't validated and handled appropriately, security breaches and privacy violations are quite likely due to the widespread and omnipresent nature of IoT [21].

Without real-time monitoring, patients' private and sensitive medical information may be altered, misused 43, or compromised [22]. This poses a grave threat to infrastructure in addition to having a devastating effect on people's lives. Apps and wearable technology might be taken over by malicious users, who could then access users' sensitive information and pose grave security and health threats [23].

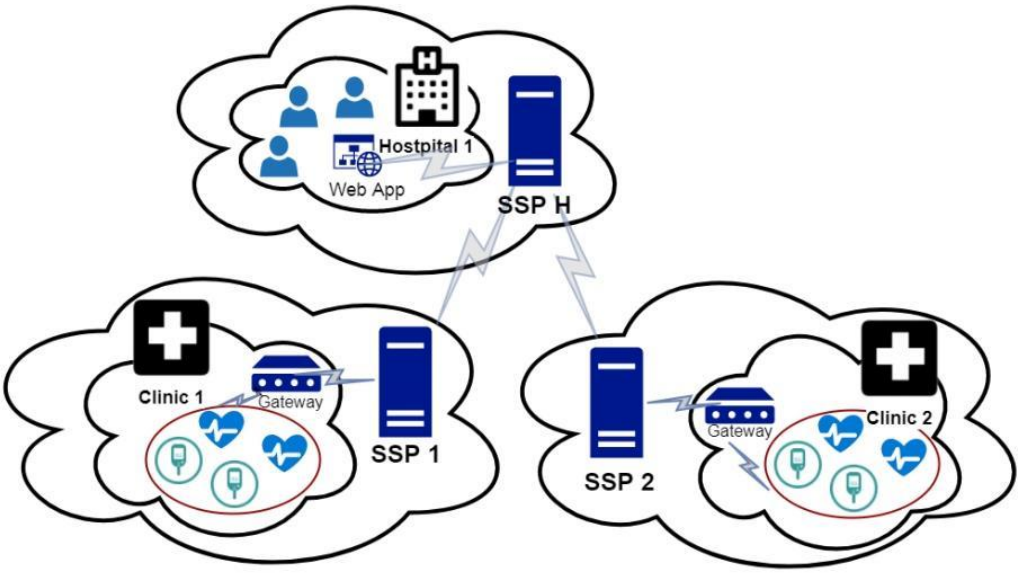

Figure 1. Reference architecture of IoT-based health care across domains

The management of passwords and access to applications and private patient data presents another difficulty [24]. When a patient's sensor gadget asks for access, for example, medical care providers are permitted to do so, but the internet connection sources may be an insecure Wi-Fi network that is readily compromised [25].

Numerous authentication approaches might be used to enable patients to confirm their identities and grant doctors' access to their internally implanted gadgets [26], but suddenly they lost consciousness and are still in severe need of medical treatment and direction [27]. Some manufacturers of IoT healthcare products offer a lifetime difficult password to managing IoT devices [28], the device documentation contains passwords that are accessible to the general public and might be used to incorrectly set the device, endangering the lives of patients [29]. Correctly establishing and executing cryptography methods in IoT health is another difficulty. Due to the ubiquitous and ongoing capabilities of the IoT, Cryptographic key management is necessary yet complex [30].

The IoT platform necessitates the use of concurrent authentication processes with real-time answers. Health information about patients should be encrypted and decrypted whenever it is judged necessary, according to HIPAA regulations regarding Transmission Security Encryption (TSE) [31]. Entities are required to create documentation of the installed encryption technology, including rules and protocols, the exchange of cryptographic key management, and limiting who has access to generate and modify cryptographic keys. Additionally, it's

important to audit and enforce policies for keeping and sharing keys that really are secret [32]–[34].

A lot of security measures have been developed to solve IoT-related issues in various apps; these plans may also be used in the healthcare industry [35]. Given that IoT comprises of constrained-devices (e.g., limited processing) [36]. The issue of secure transmission in IoT as specified by HIPAA law is inextricably linked with cryptographic methods, as are huge numbers of IoT nodes, which has expanding issues [37]. Furthermore, proper encryption management is critical in secure communication and is tied to authentication.

Due to its tiny key size and ability to meet the needs of constrained devices, symmetric key cryptography-based schemes were first the subject of in-depth research [38]. However, it has a significant scalability flaw [39]. There have also been various attempts to implement a Public Key Cryptography (PKC)-based system on restricted devices in order to overcome the scalability issue [40]. It has been demonstrated that it is possible to implement PKC with restricted hardware, particularly when utilizing ECC, which necessitates a smaller key size than RSA-based PKC [41].

However, standard PKC requires credentials, which take up more memory and are difficult to handle. A certificate less PKC system called IBC has been developed to address this issue [42]. The fundamental concept of the original IBE is as follows: initially, a central entity known as the Private Key Generator (PKG) is in charge of producing some public consideration and a core key that is kept a secret [43]. Following that, all other people that trust the specific PKG given their Identifications users can produce their own private keys using the master key [44]. With the exception that the public key can be created by any entity using a known ID, the encryption-decryption procedure can now be carried out in the same way as the conventional PKG. Due to its advantages, e.g. Some IBC-based security approaches, such as certificate less and minimal resource needs, have also been deployed for restricted devices, including Mobile Ad-hoc Networks [45]. Random strings, such as the identity of a communicating party, can be used as a public key in IBC, taking the certificate in conventional PKC place [46].

IBC plan has been put out for the Internet of Things. It is suggested to use a proxy and a key setup mechanism for two interacting entities, one of which is a restricted device [47]. Machine-to-Machine (M2M) IBC protocol design pattern was put out in reference [48].

2.2 Safety challenges and solutions. Part2

This section explores potential IoT-based hospital system design from multiple aspects [49]. Has investigated the interaction of four parties—sensor owners, sensor publishers, extended service providers, and sensor data consumers is the foundation for how IoT sensing devices work in general [50]. SO might be a business that sells sensors, a government agency, a private individual, or another SO [51].

If the SO concludes that data produced by these sensors will really be accessed on the cloud, it must define the data access policy that all SPs should implement and potential users should follow [52]. When an SDC (for example, a government agency, a business enterprise, an academic institution, or an employee) expresses interest in data exchange from a published sensor, the SP mediates the establishment of a service agreement between the SDC and the relevant SO, outlining the SO's obligations with regard to the importance and accessibility of the submitted sensing data, as well as their adherence to current standards [53].

Sensing Service Provider (SSP) is a different organization that streamlines communication between SDC and also other organizations that serve its goals, such as SO (for data accessibility, integrity, and quality), SP (for access services to sensor data), and other extended service providers (for value added services) [54]. In a scenario involving health care, SDC might be any supplier of health care services or a medical facility (such as a hospital, clinic, etc.). Those SDC in the healthcare industry may choose to adopt IoT-based hospital services for addition to their current IT infrastructure or by outsourcing it to specialist providers depending on the financial, human, and technological resources that are available [55]. Particularly for tiny medical institutes, the second choice might be more preferred (e.g. clinics, general practitioners).

From a practical standpoint, the architecture deployment strategy of an IoT-based hospital system may be done in a variety of ways . According to one of the studies, tele-EKG!, an ongoing tele-health pilot project, is done in such a way that a renowned cardiac hospital serves as the initiative's hub while also providing services to other distantly placed healthcare providers [56]. To get a diagnosis relating to the cardiac difficulties of the patients in the distant region to health care providers who lack cardiology doctors may submit the EKG test data of their patients to other cardiologist who is a member of the referring hospital using tele-EKG.

The example model is a condensed form in which SP is taken to be the SSP itself, the SO is a component of the healthcare providers (clinics one and two), and hospital 1 is the SDC.

Additionally, it is presumable that every healthcare organization hired expert providers to handle the IoT-based healthcare system (e.g., SSP 1, SSP 2 and SSP H).

According to table 1, the reference architecture will feature three PKG for each SSP domain in accordance with the planned IBC security system, which calls for PKG. PKG is only accessible to organizations that are part of its domain for security reasons. They provide public parameters and master secret keys for each domain as PKGs.

TABLE 1.
SUMMARY OF ALL ALGORITHMS IN IBE WITHOUT KEY ESCROW

Algorithm	Input	Output
Setup	1^K: a security parameter	s: system's master-key (private) params: system's public parame- ters
Extract	ID: Identity s and params	QID : public key dID : private key
Publish	params	tID : sub-private key NID : sub-public key
Encrypt	m: plaintext ID, params, NID	C: ciphertext
Decrypt	C: ciphertext dID, t, params	m' : plaintext

3. MTHODOLOGY

The definite purpose of the research projected by exploring secondary data from previously published journals, books and literature whereas, this research was primarily hold to signify Identity-Based Cryptography that is a cornerstone management strategy secures data translation between any IoT health device and any other entity from a different business or domain by using cooperative authentication and security.

4. EMPIRICAL ANALYSIS

4.1 IBE Scheme

Several researchers argued, the suggested system is based on an IBE variation without key escrow. Franklin's original IBE method uses four randomized algorithms—Setup, Extract, Encrypt, and Decrypt—while the IBE's variation without key escrow includes a fifth algorithm called Publish. The last table contains a summary of the inputs and outputs for all five methods.

And by taking note that the setup algorithm runs completely in the PKG, which may happen, for example, during system startup. As part of the Extract algorithm, the PKG gets an

AI input ID from a communicating entity. Once the algorithm is carried out in the PKG, QID is made public in a directory while dID is provided covertly to the communicating entity. The remainder of the algorithm (Publish, Encrypt, and Decrypt), with the exception of NID being one of the outcomes of the Publish process being published in a public directory, occurs in the communicating entity.

Before describing the other process in the suggested approach, namely key agreement authentication and system and device initialization. Table 2 provides definitions for the notations used in the suggested scheme.

4.2 System and Device Initialization

Framework administration is the operation performed when a gateway and a constrained device join the SSP!, although system initialization is a method performed when an SSPPKG !'s is enabled. The most important step in configuration is generating the master key and parameters, followed by making the parameters public, as mentioned in the prior section. Furthermore, the SSP PKG is dependent on it! to have a unique online identity that can be recognized by anything or anybody As a result, we recommend that the IoT Service Provider's primary identity be the domain name, to which the device identity will be attached. Even if the access points is in a different domain, having such an identifier scheme is helpful in the lookup process.

Mainly two operations must be carried out: the production and distribution of the gadget by the PKG, and the formation of sub-public and sub-private key pairs by the device itself. In theory, the device's identification and accompanying private key are distributed statically during the flashing period of the device, but the online technique may be done more dynamically. In this situation, an online approach is selected, and a secure method of providing the device's private key is suggested.

Two identical keys, KlnitReq plus KlnitRsp, which are generated one time randomly and will be useless after device initialization, are used to secure the proposed online device initialization. There are several ways to get the keys. One useful method is to register a device via a web interface. After the registration procedure, the registered device will receive a unique device identification, KlnitReq, and KlnitRsp (e.g. they can be loaded to the device by cable data after downloading from PKG). It is now able to add more human-friendly names to the unique device identification, such as the type of device (gateway, EKG, diabetes sensor, etc.). The position of the device (hospital or clinic, etc.). Then, utilizing Authenticated Encryption

with Associated Data, the device may safely ask for its identification and associated private key (AEAD). AEAD was chosen because it works quicker than a safe implementation of Hash-based Message Authentication Code (HMAC), which uses two keys for encryption and authentication, and it is more secure to fully authenticate the cipher text rather than just encrypt it. Table 2 displays the whole secure device initialization process.

TABLE 2.
DEFINITION OF USED NOTATIONS

Notation	Definition
s	Master secret key
paramsx	Public system parameter of domain x
IDi	Identity of entity i
Qi	Public key of corresponding entity i
di	Private key of corresponding entity i
Ni	Sub-public key of corresponding entity i
ti	Sub-private key of corresponding entity i
Pm	Plaintext from a message m or a result of decryption
Cm	Ciphertext, a result of encrypting message m
E(k, N, P, A)	AEAD encryption of plaintext P, using key k, nonce N and associated data A
D(k, N, C, A)	AEAD decryption of ciphertext C, using key k, nonce N and associated data A
Eij(m)	ID based encryption of message m using Qj, Nj, and ti
Dij (m)	ID based decryption of message m using Qj, Nj, and ti
Sm	Digest of message m as a result of Message Authentication Code (MAC)

4.3 Authentication Mechanism with Key Agreement:

Form three depicts a situation when the suggested authentication procedure and key agreement are used. In this example, user A of a mobile app wishes to access sensor B, which is a part of an IoTSP domain. User A and sensor B shall be referred to as A and B, respectively, moving forward for the sake of simplicity. Additionally, the access point to B for A is the IoT Server (IoTS). Since it is anticipated that the mobile app (either the app itself or the server that offers API to the app) performs action A in this situation, it is represented in form 3 as a single entity. Additionally, it may be believed that practically speaking, entities within each domain are unaware of the system parameters and sub-public keys of entities inside other domains, necessitating a lookup operation prior to encryption. Following is an explanation of the authentication technique in detail:

First, using IDIoT S = H1IoT SP (IDIoT S), where H1IoT SP is a part of paramsIoT SP, A does a search to acquire NIoT S and paramsIoT SP. For encryption, additional paramsIoT SP parameters are also utilized. Then, using QIoT s, NIoT s, and tA as keys, IDA, IDB, and

timestamp T are encrypted to generate C1. Here, T is utilized to stop a counterattack. IDA, IDIoT S, and C1 are then sent to IoTS.

IoTS will conduct a quest depending on the IDA obtained after receiving a message from A in order to acquire the parameters A and NA. After a successful search, it decrypts C1 to produce IDA, IDB, and T using dIoT S, tIoT S, and N A. Then T is validated, and IDA is checked to see whether it is comparable to the one that was received. If they are true, the procedure continues; if not, it pauses and notifies A of the problem. A message containing NB is encrypted as C2 using QA, NA, and tIoT S after successful validation, and C2 is then delivered to A. A second message containing the parameters A and NA is encrypted as C3 using QB, NB, and tIoT S before being delivered to B, letting A know that they want access to it.

After receiving C2, A uses dA, tA, and NioT S to decode it in order to produce NB. A then creates nonce A, encrypts it with IDA using QB, NB, and tA as C4 before sending it to B.

B decrypts C3 after receiving it from IoTS in order to get the parameters M A and NA utilizing dB, tB, and NioT S.

B decrypts C4 using dB, tB, and NA after receiving it from A in order to produce nonceA. Then, using a key derivation function, such as an HMAC-based Key Derivation Function, B creates nonceB and uses it, together with nonceA and IDB, to create the shared secret key with A, kBA (HKDF). After that, IDB and nonceB are encrypted using QA, NA, and tB as C5, and a digital S1 is made from a message made up of IDB, IDA, and nonceA with key KBA using a message authentication code like HMAC. IDB, IDA, C5, and S1 are then sent to A.

A receives C5 and S1, decrypts C5 using dA, tA, and NB to derive nonceB, and then generates KBA using nonceA, nonceB, and ID. Next, using the newly constructed kBA, another S/ is formed in the same manner that B did it, and it is then validated against the received S1. Following S1's verification, S2 is produced using IDA, IDB, and nonceA using kBA and delivered to B.

S2 is then validated by b when it has been received. Both A and B will use kBA as their shared secret key after successful verification.

User A and sensor B are ultimately together are authenticated. Additionally, they may communicate privately and securely using symmetric key encryption, such as Advanced Encryption Standard (AES), which has kBA and is more compact than public key encryption.

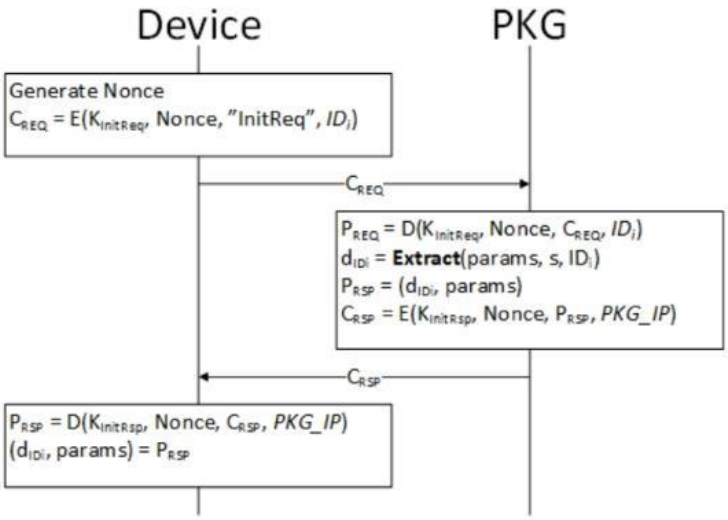

Figure 2. Device initialization protocol in a SSP! Domain

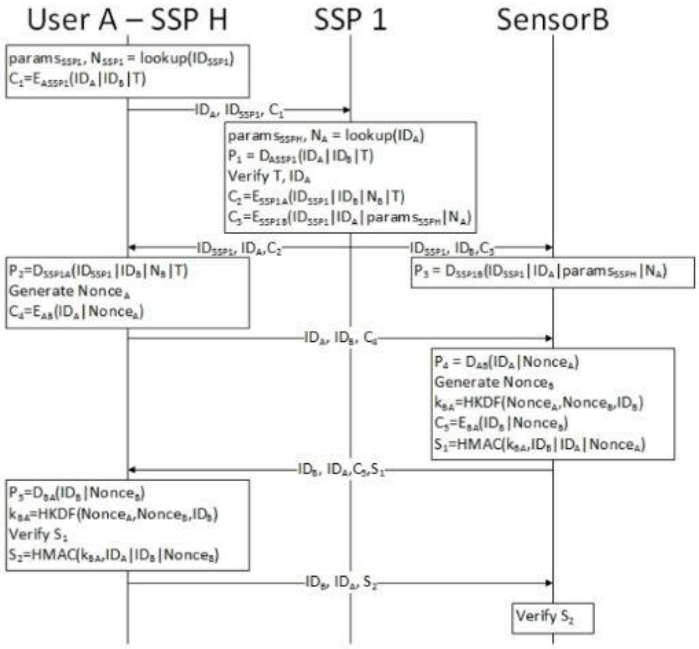

Figure 3. Authentication mechanism with entity in different domain

5. RESULTS AND DISCUSSION

The security capabilities of the suggested approach are discussed in this chapter. The threat model used for the security study is provided first. The suggested scheme's security aspects are next examined. Finally, a discussion on mutual authentication's security is had.

5.1 Risk Model

Every message sent through the system is eavesdropped on by an outside attacker who then replays the previous message to the receiver, breaks up the eavesdropped message into smaller pieces, reassembles the pieces into a new message, and sends the new message to any legal entity. The attacker can also decrypt ciphertext if they have access to the corresponding key, modify the decrypted plaintext, and forge messages using the public key of a legal entity.

Compromised equipment, such one that can perform all actions an outside attacker might, uses its own private key, which was given with MSP, to decode intercepted messages or create fake ones. A compromised SSP that uses its own private key to decode intercepted messages or create fake messages and is able to do any action an outside attacker could.

- *Security Feature of The Proposed Scheme*

When a communication is encrypted, it is authenticated: Sender I must use ti to encrypt the message before sending it to receiver j, and the recipient must use Ni to decode the message. The message could only be properly encrypted and decrypted with the right (ti,Ni) combination. This indicates that the recipient could only decode the message by the matching Ni if the communication was encrypted by an authorized sender i. Therefore, the encryption serves as the message's authentication, and no more signatures are required.

The key escrow issue is solved by using dj and tj when a receiver j wishes to decode a message. The receiver is the sole party with knowledge of the dj, SSP, and tj. The message could therefore only be decoded by the recipient because to the tj even if the SSP is hacked or the private key dj is exposed. The primary escrow issue is thus resolved by the presence of tj. Likewise, the update of data strengthens the authentication scheme's security.

- *Mutual Authentication*

The authentication technique enables mutual authentication between a hospital user, a medical sensor, and the SSP1! The SSP1! verifies the hospital user's ID. The SSP1 and its associated sub-public key NID could only decipher messages encrypted by authorized hospital users. Additionally, the sub-secret key tID makes sure that only the authorized mobile user may authenticate a message with encryption, and that only the target sensor can decode a message and vice versa.

6. CONCLUSION

IoMT security and privacy assurance is a really difficult task. The fact that IoT is mostly used to link patients with medical institutions or among a number of healthcare providers spread across several sectors with various levels of trust authority makes it more difficult. An IBC-based system has been put forth for the purpose of securing communication in IoMT across several domains. The key contributions are the IBE-based key-escrow-free authentication mechanism, the mechanism to look up IBE system parameters in other domains, the mechanism to generate shared secret keys to secure communication of the presentation of the mutual authentication.

A cryptographic identity might be used alternatively of a plain identity to facilitate verification and increase identity security, but this is still up for debate. In order to take into account more stakeholders as described in the suggested model, an extension of the proposed scheme with an expanded IoT-based health care system architecture needs to be taken into consideration. To test the effectiveness and practical viability of the suggested method, it will also be implemented in a prototype or genuine IoT system.

REFERENCES

[1] S. R. Guntur, R. R. Gorrepati, and V. R. Dirisala, "Internet of Medical Things," *Med. Big Data Internet Med. Things*, vol. 4, no. 6, pp. 271–297, 2018, doi: 10.1201/9781351030380-11.

[2] T. M. Ghazal *et al.*, "AI-Based Prediction of Capital Structure: Performance Comparison of ANN SVM and LR Models," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–13, 2022, doi: 10.1155/2022/8334927.

[3] D. Miller, "The Best Practice of Teach Computer Science Students to Use Paper Prototyping," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 42–63, 2021, doi: 10.54489/ijtim.v1i2.17.

[4] N. Nanayakkara, M. Halgamuge, and A. Syed, "Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review," 2019.

[5] T. Eli, "Students` Perspectives on the Use of Innovative and Interactive Teaching Methods at the University of Nouakchott Al Aasriya, Mauritania: English Department as a Case Study," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 90–104, 2021, doi: 10.54489/ijtim.v1i2.21.

[6] H. M. Alzoubi *et al.*, "Empirical linkages between ICT, tourism, and trade towards sustainable environment: evidence from BRICS countries," 2022, doi: 10.1080/1331677X.2022.2127417.

[7] A. A. Kashif, B. Bakhtawar, A. Akhtar, S. Akhtar, N. Aziz, and M. S. Javeid, "Treatment Response Prediction in Hepatitis C Patients using Machine Learning Techniques," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 79–89, 2021, doi: 10.54489/ijtim.v1i2.24.

[8] H. M. Alzoubi, J. R. Hanaysha, M. E. Al-Shaikh, and S. Joghee, "Impact of Innovation Capabilities on Business Sustainability in Small and Medium Enterprises," *FIIB Bus. Rev.*, vol. 11, no. 1, pp. 67–78, 2022, doi: 10.1177/23197145211042232.

[9] A. Akhtar, S. Akhtar, B. Bakhtawar, A. A. Kashif, N. Aziz, and M. S. Javeid, "COVID-19 Detection from CBC using Machine Learning Techniques," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 65–78, 2021, doi: 10.54489/ijtim.v1i2.22.

[10] T. Mehmood, "Does Information Technology Competencies and Fleet Management Practices lead to Effective Service Delivery?," *Empir. Evid. from E-Commerce Ind.*, vol. 1, no. 2, pp. 14–41, 2021.

[11] N. Alsharari, "Integrating Blockchain Technology with Internet of things to Efficiency," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 2, pp. 01–13, 2021, doi: 10.54489/ijtim.v1i2.25.

[12] R. Bose, H. Mondal, I. Sarkar, and S. Roy, "DESIGN OF SMART INVENTORY MANAGEMENT SYSTEM FOR," *e-Prime - Adv. Electr. Eng. Electron. Energy*, p. 100051, 2022, doi: 10.1016/j.prime.2022.100051.

[13] Vorobeva Victoria, "Impact of Process Visibility and Work Stress To Improve Service Quality: Empirical Evidence From Dubai Retail Industry," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.59.

[14] H. M. Alzoubi, H. Elrehail, J. R. Hanaysha, A. Al-Gasaymeh, and R. Al-Adaileh, "The Role of Supply Chain Integration and Agile Practices in Improving Lead Time During the COVID-19 Crisis," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 13, no. 1, pp. 1–11, 2022, doi: 10.4018/IJSSMET.290348.

[15] T. Eli and Lalla Aisha Sidi Hamou, "Investigating the Factors That Influence Students` Choice of English Studies As a Major: the Case of University of Nouakchott Al Aasriya, Mauritania," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.62.

[16] M. Alazab, S. Alhyari, A. Awajan, and A. B. Abdallah, "Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance," *Cluster Comput.*, vol. 24, no. 1, pp. 83–101, 2021, doi: 10.1007/s10586-020-03200-4.

[17] John Kasem and Anwar Al-Gasaymeh, "a Cointegration Analysis for the Validity of Purchasing Power Parity: Evidence From Middle East Countries," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.60.

[18] H. M. Alzoubi and R. Yanamandra, "Empirical Investigation of Mediating Role of Six Sigma Approach in Rationalizing the COQ in Service Organizations," *Oper. Supply Chain Manag. An Int. J.*, vol. 15, no. 1, pp. 2579–9363, 2022.

[19] G. Ahmed and Nabeel Al Amiri, "the Transformational Leadership of the Founding Leaders of the United Arab Emirates: Sheikh Zayed Bin Sultan Al Nahyan and Sheikh Rashid Bin Saeed Al Maktoum," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.58.

[20] G. M. Qasaimeh and H. E. Jaradeh, "The Impact of Artificial Intelligence on the effective applying of Cyber Governance in Jordanian Banks," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.

[21] E. Al Alkeem, D. Shehada, C. Y. Yeun, M. J. Zemerly, and J. Hu, "New secure healthcare system using cloud of things," in *Cluster Computing, , Vol. 20, No. 3*, 2017, pp. 2211–2229.

[22] N. Alsharari, "the Implementation of Enterprise Resource Planning (Erp) in the United Arab Emirates: a Case of Musanada Corporation," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijtim.v2i1.57.

[23] H. M. Alzoubi, M. In'airat, and G. Ahmed, "Investigating the impact of total quality management practices and Six Sigma processes to enhance the quality and reduce the cost of quality: the case of Dubai," *Int. J. Bus. Excell.*, vol. 27, no. 1, pp. 94–109, 2022, doi: 10.1504/IJBEX.2022.123036.

[24] Asem Alzoubi, "Machine Learning for Intelligent Energy Consumption in Smart Homes," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.75.

[25] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Khosravi, M. R. Ghalib, and A. Shankar, "Big data analytics to identify illegal activities on Bitcoin Blockchain for IoMT," *Pers. Ubiquitous Comput.*, 2021, doi: 10.1007/s00779-021-01562-z.

[26] Nada Ratkovic, "Improving Home Security Using Blockchain," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.72.

[27] H. M. Alzoubi *et al.*, "Fusion-based supply chain collaboration using machine learning techniques," *Intell. Autom. Soft Comput.*, vol. 31, no. 3, pp. 1671–1687, 2022, doi: 10.32604/IASC.2022.019892.

[28] Maged Farouk, "Studying Human Robot Interaction and Its Characteristics," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.73.

[29] M. El Khatib, A. Al Mulla, and W. Al Ketbi, "The Role of Blockchain in E-Governance and Decision-Making in Project and Program Management," *Adv. Internet Things*, vol. 12, no. 03, pp. 88–109, 2022, doi: 10.4236/ait.2022.123006.

[30] H. M. Alzoubi, J. Hanaysha, and M. Al-Shaikh, "Importance of Marketing Mix Elements in Determining Consumer Purchase Decision in the Retail Market," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 12, pp. 56–72, 2021, doi: 10.4018/IJSSMET.2021110104.

[31] Neyara Radwan, "the Internet'S Role in Undermining the Credibility of the Healthcare Industry," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.74.

[32] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today Proc.*, vol. 37, no. Part 2, pp. 2653–2659, 2020, doi: 10.1016/j.matpr.2020.08.519.

[33] H. M. Alzoubi, A. U. Rehman, R. M. Saleem, Z. Shafi, M. Imran, and M. Pradhan, "Analysis of Income on the Basis of Occupation using Data Mining," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–4. doi: 10.1109/ICBATS54253.2022.9759040.

[34] Edward Probir Mondol, "the Role of Vr Games To Minimize the Obesity of Video Gamers," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.70.

[35] H. M. Alzoubi and R. Aziz, "Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation," *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 2, p. 130, 2021, doi: 10.3390/joitmc7020130.

[36] Saad Masood Butt, "Management and Treatment of Type 2 Diabetes," *Int. J. Comput. Inf. Manuf.*, vol. 2, no. 1, p. 1, 2022, doi: 10.54489/ijcim.v2i1.71.

[37] H. M. Alzoubi *et al.*, "Modelling supply chain information collaboration empowered with machine learning technique," *Intell. Autom. Soft Comput.*, vol. 30, no. 1, pp. 243–257, 2021, doi: 10.32604/iasc.2021.018983.

[38] F. Del and G. Solfa, "IMPACTS OF CYBER SECURITY AND SUPPLY CHAIN RISK ON DIGITAL OPERATIONS: EVIDENCE FROM THE UAE PHARMACEUTICAL INDUSTRY Federico Del Giorgio Solfa," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 18–32, 2022.

[39] H. M. Alzoubi, M. Vij, A. Vij, and J. R. Hanaysha, "What leads guests to satisfaction and loyalty in UAE five-star hotels? AHP analysis to service quality dimensions," *Enlightening Tour.*, vol. 11, no. 1, pp. 102–135, 2021.

[40] Nasim, S. F., M. R. Ali, and U. Kulsoom, "Artificial Intelligence Incidents & Ethics A Narrative Review. International Journal of Technology, Innovation and Management," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 2, pp. 52–64, 2022.

[41] H. M. Alzoubi, M. Alnuaimi, D. Ajelat, and A. A. Alzoubi, "Towards intelligent organisations: An empirical investigation of learning orientation's role in technical innovation," *Int. J. Innov. Learn.*, vol. 29, no. 2, pp. 207–221, 2021.

[42] B. Amrani, A. Z., Urquia, I., & Vallespir, "INDUSTRY 4.0 TECHNOLOGIES AND LEAN

PRODUCTION COMBINATION: A STRATEGIC METHODOLOGY BASED ON LINKS QUANTIFICATION Anne Zouggar Amrani, Ilse Urquia Ortega, and Bruno Vallespir," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 33–51, 2022.

[43] H. M. Alzoubi, S. Joghee, and A. R. Dubey, "Decisions effectiveness of FDI investment biases at real estate industry: Empirical evidence from Dubai smart city projects," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 3499–3503, 2020.

[44] G. Al-Naymat, H. Hussain, M. Al-Kasassbeh, and N. Al-Dmour, "Accurate detection of network anomalies within SNMP-MIB data set using deep learning," *Int. J. Comput. Appl. Technol.*, vol. 66, no. 1, pp. 74–85, 2021.

[45] S. Goria, "A DECK OF CARDS TO HELP TRACK DESIGN TRENDS TO ASSIST THE," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 1–17, 2022.

[46] H. M. Alzoubi, G. Ahmed, A. Al-Gasaymeh, and B. Al Kurdi, "Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration," *Manag. Sci. Lett.*, vol. 10, no. 3, pp. 703–708, 2020, doi: 10.5267/j.msl.2019.9.008.

[47] P. S. Ghosh, S., & Aithal, "BEHAVIOUR OF INVESTMENT RETURNS IN THE DISINVESTMENT," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 65–79, 2022.

[48] H. M. Alzoubi *et al.*, "Digital Transformation and SMART-The Analytics factor," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–11. doi: 10.1109/ICBATS54253.2022.9759084.

[49] H. Alzoubi and M. & Alnazer, N., Alnuaimi, "Analyzing the Appropriate Cognitive Styles and its effect on Strategic Innovation in Jordanian Universities," *Int. J. Bus. Excell.*, vol. 13, no. 1, pp. 127–140, 2017.

[50] S. Akhtar, A., Bakhtawar, B., & Akhtar, "EXTREME PROGRAMMING VS SCRUM: A COMPARISON OF AGILE MODELS Asma Akhtar, Birra Bakhtawar, Samia Akhtar," *Int. J. Technol. Innov. Manag. (IJTIM), 2(2).*, vol. 2, no. 2, pp. 80–96, 2022.

[51] T. M. Ghazal *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, 2022, doi: 10.1049/cmu2.12301.

[52] H. M. Alzoubi *et al.*, "Securing Smart Cities Using Blockchain Technology," in *2022 1st International Conference on AI in Cybersecurity (ICAIC*, 2022, pp. 1–4. doi: 10.1109/icaic53980.2022.9896971.

[53] H. Alzoubi and G. Ahmed, "Do TQM practices improve organisational success? A case study of electronics industry in the UAE," *Int. J. Econ. Bus. Res.*, vol. 17, no. 4, pp. 459–472, 2019, doi: 10.1504/IJEBR.2019.099975.

[54] H. M. Alzoubi and R. Yanamandra, "Investigating the mediating role of Information Sharing Strategy on Agile Supply Chain in Supply Chain Performance," *Uncertain Supply Chain Manag.*, vol. 8, no. 2, pp. 273–284, 2020.

[55] M. Abu-Arqoub, G. Issa, A. E. Banna, and H. Saadeh, "Interactive Multimedia-Based Educational System for Children Using Interactive Book with Augmented Reality," *J. Comput. Sci.*, vol. 15, no. 11, pp. 1648–1658, 2020, doi: 10.3844/jcssp.2019.1648.1658.

[56] H. M. Alzoubi, A. Ali, A. W. Septyanto, I. Chaudhary, H. A. Hamadi, and Z. F. Khan, "Applied Artificial Intelligence as Event Horizon Of Cyber Security," in *2022 International Conference on Business Analytics for Technology and Security (ICBATS*, 2022, pp. 1–7. doi: 10.1109/ICBATS54253.2022.9759076.