Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Check for updates

Internet of medical things: Prospects, challenges and future research directions

Abraham Isiaho * and Kelvin Kabeti Omieno

Kaimosi Friends University College, Kaimosi, Kenya.

Global Journal of Engineering and Technology Advances, 2022, 12(1), 012–024

Publication history: Received on 02 June 2022; revised on 05 July 2022; accepted on 07 July 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.12.1.0108

Abstract

The internet of medical things has been developed to facilitate remote monitoring of the patients as well as the elderly. Unfortunately, the communication between the remote patients and the medical doctors is the open wireless channels. Therefore, the data transmitted can be eavesdropped, intercepted, replayed or modified. This poses serious challenges to patient privacy as well as endangering patient life. To curb this, numerous schemes have been put forward by various researchers over the recent past. In this paper, we provide an extensive review of these schemes in an effort to identify any gaps. Consequently, we show that the current security and privacy preservation schemes have many challenges that render the communication process insecure or inefficient. As such, we offer some suggestions for the requirements of an ideal security technique that will not only be efficient but also provably secure.

Keywords: IoMT; Privacy; Security; Authentication; 5G; Efficiency

1. Introduction

The Internet of Things (IoT) involves the interconnection of smart devices to boost the exchange of information among these devices [1]. In most cases, the interconnection of these smart devices is used to provide remote monitoring of the environment where these devices are deployed. As such, they have found applications in areas such as healthcare [2], military, smart homes, smart power grid systems [3], fire monitoring and traffic management among others. In the healthcare system, IoT offer real-time healthcare monitoring of the patients where the sensors are implanted in the body or placed in the vicinity of the patient. In so doing, it becomes possible to monitor parameters such as body temperature, heart rate, and blood pressure and insulin levels. Therefore, IoT presents a more convenient and efficient way for remotely accessing medical services for the patients. It also facilitates remote health monitoring of the patients by the doctors, physicians and nurses over the Internet as shown in Fig.1

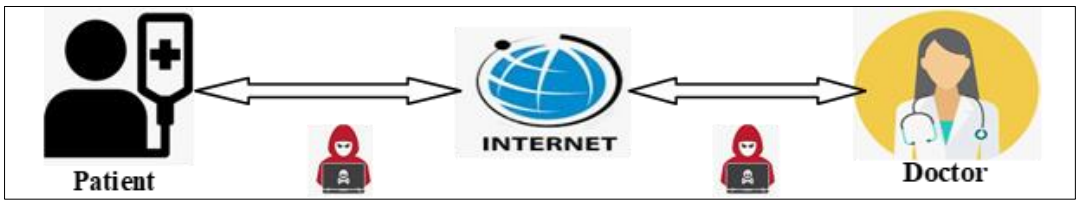

Figure 1 Typical IoMT Communication

As shown in Fig.1, the communication between the remote patient and the doctor takes place over the public internet. Here, the attackers located between the patient and the doctor can intercept all the exchanged data. In addition, attacks

*Corresponding author: Abraham Isiaho
Kaimosi Friends University College, Kaimosi, Kenya.

such as eavesdropping, packet replays, impersonation, man-in-the-middle, de-synchronization, dictionary and offline password guessing are possible.

As explained in [4] Tele-care Medical Information System (TMIS) plays a critical role for people with disabilities or diseases that may render physical hospital attendance for routine checkups extremely difficult. As such, TMIS saves not only time but also the associated costs. The main elements in any IoT-healthcare systems include the patients (users), the wireless communication channel, the medical server as well as the medical staff. In this environment, the medical server facilitates remote access of the medical services by all registered patients over some mobile network or internet [5], [6]. As pointed out in [7], Internet of Medical Things (IoMT) is a collection of all the medical devices and its applications that are linked to healthcare IT systems through a well-established computer network. In the past few years, electronic health has emerged as the most important service model that has attracted the attention of most researchers worldwide. The healthcare revolution called "smart health" has greatly made it possible for medical staff to monitor and diagnose patients remotely for physical and emotional ailments. It is also possible for medical staff to perform some certain kinds of surgery. IoMT has been used as an effective tool for patient care during the COVID-19 pandemic.

The devices utilized in IoMT ranges from sensors [8] which are connected close to the patient's body with aid of a network referred to as wireless body area network (WBAN). These sensors are used for real time healthcare monitoring of patients as well as providing support. The sensors are portable and very small in size to facilitate intercommunication between patient, actuators and health care personnel. The sensors exist in various forms: wearable sensors which are worn by patients; as well as implanted sensors which are inserted in the patient body to deal with disease such as blood oxygen saturator which affects elderly people. These sensors provide enormous services to patients and also elderly people who need care while at home. The sensors collect vital information and send them to the hospital through some wirelessly channels [9].

Different types of WBANs sensors can perceive and collect important environmental and physiological information from the human body. Thereafter, this information is immediately forwarded to the remote control centers using personal terminals, where they are analyzed and deployed to address various patient requirements. In case of an emergency such as heart failure, the sensors implanted in body will send information to hospital and doctor or nurse will respond to this emergency without hesitation. Other applications of internet of medical things include monitoring of elder people and also disabled people at home who don't need to be hospitalized. In addition, they can be utilized for the monitoring of the initial stage of disease before detailed diagnosis by responsible doctors.

Although IoMT offers cost reduction and efficiency [10], security and privacy are considered key concerns in these systems due to communication over the insecure wireless channels. Since these networks convey data that deals with human life, it is paramount that confidentiality be upheld [11]. This implies that an intruder should not be permitted to listen to transmission line and access the information being transmitted. This still remains a challenge since information exchanged over the open communication channels can be eavesdropped by an adversary [12]. In addition, the communication is vulnerable to many attacks such as cloning, replaying, and traceability. Replay attacks are particularly serious, where a valid data transmitted can be maliciously or fraudulently delayed or repeated .This attack can cause a delay in response, hence endangering life of a patient. For instance, a doctor can repeat an instruction to the actuator to administer excess insulin, leading to adverse effect or even death to patient [13]. Key compromise and impersonation attacks are also extremely dangerous attacks in WBAN. For instance, an adversary after successful tapping thorough the transmission can impersonate a doctor and provide wrong guidelines which can compromise the life of a patient.

To address these threats, there is need to uphold data confidentiality, integrity and authentication. Unfortunately, IoMT uses various concepts of technology such as Internet of Service (IoS) [14] and cyber-physical systems (CPSs), which are exposed to attackers. Due to enormous data processing in IoMT, conventional data security and authentication mechanisms of cloud computing are no longer suitable for data security in IoMT edge paradigm. As such, achieving perfect security in IoMT platform is a big challenge. The major contributions of this paper include the following:

- An extensive review of the current security techniques for the internet of medical things is provided.
- Elaborate discussion on some of the pertinent challenges of the conventional security schemes that impede their applicability is offered.
- Based on the identified shortcomings, probable research gaps are identified. Thereafter, feasible solutions are provided.

The rest of this article is structured as follows: Section 2 presents related work while Section 3 discusses the key findings. On the other hand, requirements for the proposed scheme are described in Section 4 while future research directions are explained in Section 5. Towards the end of this paper, Section 6 gives the conclusions of this paper.

2. Related Work

A myriad of privacy and security enhancement techniques have been presented by many researchers. In [15], a secure and mutual RFID-based tag authentication scheme is introduced to offer protection in the medical environment. This scheme is shown to be resilient against many attacks such as packet replays, de-synchronization, forgery and traceability. Unfortunately, this scheme lacks of mutual authentication and is venerable to stolen reader attacks [16]. To address these attacks, the authors in [13] have introduced a lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. This protocol is shown to offer perfect forward secrecy and resistance to the key compromise, impersonation and session-specific temporary information attack. However, packet replay attacks are never addressed in this technique. This is a serious attack since an adversary can make several requests commanding actuators to repeat the task of pumping drugs to patients, leading to overdose. To address this issue, the scheme developed in [17] can be deployed. In addition, the scheme in [18] that is based on Elliptic Curve Cryptography (ECC) can also be utilized. This is due to its resilience against attacks such as packet replays, Denial of Service (DoS), impersonation, spoofing, Man-in-the-Middle (MitM), tracking, cloning, de-synchronization and location tracking. Unfortunately, this scheme cannot protect against tag identity leakage attacks [19].

In terms of efficiency, the smart card and password-based protocol developed in [20] is demonstrated to be lightweight and hence applicable to IoT sensors. Although this scheme preserves confidentiality, it is vulnerable to smart card loss and offline password guessing attacks. Similarly, an efficient ECC based scheme is presented in [21] while another ultra-lightweight authentication method is developed in [2]. The authors in [21] show that their protocol is resistant against MitM, packet replays, impersonation, forgery and privileged insider attacks. However, the provable security [22] component of this protocol is missing. On the other hand, the scheme in [2] is shown to be robust against many security attacks and also offers information privacy. Its formal security analysis is executed using BAN logic and Scyther tool, hence addresses the issues in [21].

To address security challenges in [15], an identity-based authentication protocol is presented in [16]. This scheme not only offers mutual authentication but also resilience against stolen reader, de-synchronization and packet replay attacks. However, this protocol is still susceptible to traceability attacks and has integrity problems [23]. As explained in [24], Radio Frequency Identification (RFID) presents one of the most viable technologies that can be deployed unique identification of communicating entities. For instance, this technology can be applied in health care systems for medicine and location tracking of patients [25]. Here, the communication between the tag and reader is executed over wireless channel. Unfortunately, the use of RFID raises severe security and privacy concerns due to the transmission of identities in plaintext [26]. To address this issue, the two-factor user verification protocol is developed in [27] using smart cards and passwords. The author claims that this scheme is immune to stolen verifier and impersonation attacks. However, it cannot withstand node imitation attacks. This issue is addressed by the RFID based authentication protocol in [28] where authentication is carried out using hash-based cryptography. Nevertheless, this protocol cannot withstand forgery and MitM attacks [29], [30].

Based on El-Gamal cryptosystem, a privacy preservation protocol is developed in [31] for TMIS systems, while an ECC based scheme is introduced in [32]. It is shown that the protocol in [31] withstands de-synchronization, location tracking, packet replays, impersonation and DoS attacks. On its part, the technique in [32] effectively addresses the security challenges in [33]. Nevertheless, the protocol in [32] is not immune against DoS, location tracking and cloning attacks [34], [35]. These challenges are addressed by the joint verification schemes presented in [36], [37] and [38]. Unfortunately, the protocols in [37] and [38] are still susceptible to tag impersonation, tracking and reader impersonation attacks [39]. To prevent non-repudiation attacks, authors in [40] have introduced a blockchain based technique for message verification in an IoT environment. However, blockchain technology has high computation and storage overheads [41].

To offer one-to-many authentication in Wireless Body Area Networks (WBANs), a lightweight multilayer scheme is developed in [42]. This protocol is demonstrated to be secure and robust when adding or deleting group members. In addition, it is shown to incur fewer overheads when generating the group key and authentication among group members. Similarly, the hop-by-hop verification protocol in [43] is lightweight and also preserves user confidentiality. Unfortunately, the scheme in [42] can be compromised if one or more group members turn out to be malicious [44]. In addition, this scheme has high computation complexities due to ECC point multiplication operations. This can make the sensors implanted in the patient body not to last as expected [45], [46]. However, the scheme developed in [47] is truly

lightweight and hence can help preserve sensor battery power. To offer forward key secrecy, authors in [48] have developed an identity-based scheme for message verification in health-care environment. Unfortunately, this protocol is susceptible to key compromise attacks that will facilitate adversarial tag secret recovery [49], [50], [51]. In addition, identity-based protocols have key escrow issues [52]. Another secure scheme based on ECC is presented in [53] that is shown to be robust against many attack vectors. However, this scheme is cannot withstand tag and server impersonation attacks and hence privacy is not assured. In addition, it fails to provide both backward and forward key secrecy [54]-[56]. On the other hand, single-use signature based scheme has been developed in [57] while a joint verification scheme has been presented in [58] based on symmetric and biometric [59] encoding techniques. To offer sufficient security protection, authors in [60] and [61] have developed bilinear pairing based authentication protocols. Although the scheme in [60] offers anonymity and forward key secrecy, it is vulnerable to impersonation attacks. In addition, the bilinear pairing operations incur high computation overheads [62]. Similarly, bilinear pairing based schemes presented in [63], [64] and [65] have high storage and computation complexities.

To mitigate security issues, cooperation techniques are presented in [66]. Unfortunately, performance and reliability factors are not optimal in this protocol. In addition, the protocol faced issues with failure in main master nodes that can lead to barrier in flow of information among nodes. There is therefore need to incorporate proactive protocol that will ensure there is cooperation between parameters. Moreover, there is need for the selection of secondary coordinator algorithm when main master nodes fails or overloaded. The protocol developed in [67] does not require any master nodes and can therefore alleviate the issues with the protocol developed in [66]. Similarly, an Elliptic curve Diffie-Hellman based key exchange protocol in [68] can address the issues in [66]. Unfortunately, the scheme presented in [68] has scalability problems [69]. In addition, it is vulnerable to de-synchronization attacks [70]. The joint verification scheme in [71] as well as the authentication protocol in [72] can addressthe challenges in [68] in addition to upholding information privacy. Based on the Public Key Infrastructure (PKI), a digital certificates based scheme is presented in [73]. However, PKI based schemes have high computation and communication overheads [74]. The mutual authentication protocols in [75] and [76] can address the challenges in [73] due to their lightweight nature.

To boost user confidentiality as well as backward and forward key privacy, verification procedures are presented in [77] and [78]. Unfortunately, the protocol in [77] is vulnerable to forwarding untraceability problem [79]. On the other hand, an efficient and lightweight key agreement and authentication is developed in [80]. This algorithm addresses security challenges such as compromise, packet replays and sensor node impersonation attacks. It also provided forward and backward key secrecy. However, the computational complexity of this approach is too high and hence it incurs high energy consumption. To address this challenge, a lightweight access control authentication protocol is introduced in [81]. This protocol utilizes ECC and Physically Unclonable Function (PUF) to establish a secure authentication between tag and server. However, PUF-based schemes have stability issues [82]. Group-based authentication protocols in [83] and [84] can potentially solve stability issues in [81] in addition to offering backward and forward key privacy. Moreover, asymmetric key protocol is negotiated among the communicating entities that is used to offer user confidentiality. However, these protocols incur high computation and communication complexities due to the deployment of asymmetric key cryptography [85]. This challenge can be solved by the lightweight schemes developed in [86] and [90]. Unfortunately, the protocol in [86] is vulnerable to active tracking attack [87]-[89]. In [90], the tag generates random nonces for key updating operation to ensure strong forward untraceability. However, this scheme incurs very high computation overheads. On their part, the authors in [91] present a two way IoT verification technique based on RSA and Trusted Platform Module (TPM).

3. Results

A myriad of security, privacy as well as performance challenges have been identified in virtually all the current security techniques for IoMT. Some of these challenges include DoS, MitM, packet replays, instability, key escrow, lack of mutual authentication, stolen smart card attacks, identity leakage, offline password guessing, traceability, node imitation, forgery, cloning, tag impersonation, key compromise, lack of both backward and forward key secrecy, de-synchronization, as well as high computation, communication and storage overheads. Table 1 below presents a summary of these schemes and their challenges.

It is evident from Table1 that most of the current schemes have many security, privacy and performance challenges that impede their deployment in IoMT. Based on the discussions above, it is also clear that majority of the current IoMT schemes deploy ECC [92]. In addition, some of them also utilize the Rivest–Shamir–Adleman (RSA) algorithm to execute authentication. Unfortunately, cryptographic algorithms such as RSA and signature algorithms such as SHA-1 are computationally complicated [93]. This is due to their high memory and power requirements during the real-time securing of healthcare data. Therefore, the design of these algorithms renders them impractical in the real-time

healthcare applications where the sensors are resource constrained. Table2 presents the taxonomy of the challenges of the conventional security technologies that are frequently deployed in IoMT.

Table 1 Summary of Challenges of Current IoMT Schemes

Scheme	**Challenges**
Srivastava et al. [15]	lacks of mutual authentication and is venerable to stolen reader attacks
Fotouhi et al. [13]	Packet replay attacks are never addressed
Jin et al. [18]	Cannot protect against tag identity leakage attacks
Kumar et al. [20]	Vulnerable to smart card loss and offline password guessing attacks
Noori et al. [21]	Provable security is missing
Li et al. [16]	Susceptible to traceability attacks and has integrity problems
Das [27]	Cannot withstand node imitation attacks
Yang et al. [28]	Vulnerable to forgery and MitM attacks
Shen et al. [32]	Susceptible to DoS, location tracking and cloning attacks
Fan et al. [37], Benssalah et al. [38]	Susceptible to tag impersonation, tracking and reader impersonation attacks
Chen et al. [39]	Incurs high computation and storage overheads
Jian et al. [42]	Insecure when some group members are malicious; incurs high computation complexities
Liao and Hsiao [48]	Susceptible to key compromise attacks; has key escrow issues
Chou [53]	Vulnerable to tag and server impersonation attacks; cannot offer backward and forward key secrecy
Jiang et al. [60]	Susceptible to impersonation attacks; incur high computation overheads
Jan et al. [36], Shao et al. [63], He et al. [64], Zhao et al. [65]	Incur high computation overheads
Haider, et al. [66]	Performance and reliability factors are not optimal
Alamr et al. [68]	Has scalability problems; vulnerable to de-synchronization attacks
Karthikeyan et al. [73]	Has high computation and communication overheads
Farash et al. [77]	Vulnerable to forwarding untraceability problem
Rehman [80]	Has high computational complexity
Xiao et al. [81]	Has stability issues
Lai et al. [83], Lai et al. [84]	Have high computation and communication complexities
He et al. [86]	Vulnerable to active tracking attack
Zhou et al. [90]	Incurs very high computation overheads
Durairaj et al. [92], Kothmayr et al. [91]	Are computationally complicated

Table 2 Challenges of Current Security Technologies

Security technology	Challenges
Public key cryptography	High computation complexities
Blockchain	Extensive storage and computation overheads
Bilinear pairings	High computation complexities
RSA	Computationally complicated
PUF	Instability
ECC point multiplication	High processing costs
One-way hashing	Collision attacks
Trusted authority based	Single point of failure
Identity-based	Key escrow
Passwords	Offline password guessing, dictionary, brute force
Smartcards	Smartcard loss attacks
RFID	Confidentiality breaches

As shown in Table 2, most of the legacy technologies for securing IoMT communications have security and performance challenges. Therefore, a need arises for novel security technologies that will provide sufficient levels of security and privacy at optimal performance levels.

4. Requirements for the Proposed Scheme

IoT devices are exponentially maturing, especially with the development of new cellular network technologies such as 5G and 6G networks. The ultra-low communication latencies coupled with high capacities have facilitated the deployment of these technologies as the backbone of most of the IoMT communications. This has in turn made patient life better, easier, and more comfortable. As the service providers rush to fill the ever increasing demands for IoMT devices, security and privacy issues are normally after-thoughts. There is therefore need to incorporate security at every level during the development of smart health devices. The revolution of sensing devices as well as networking components call for more innovative solutions to achieve high levels of security and privacy. Fig.2 gives the network architecture of the proposed secure communication in an IoMT environment. As shown in Fig.2, the link between the patient and the doctor is the cellular technologies such as 5G, Beyond 5G (B5G) or 6G. To safe on battery power, most of the processing is offloaded to the cloud. It is also evident that the public channel between the patient and the doctor is sufficiently protected by some agreed upon session keys. In this communication environment, the following security requirements are necessary.

- Measure patient data exchanged between the doctor and the patient must be enciphered to protect their confidentiality and integrity.

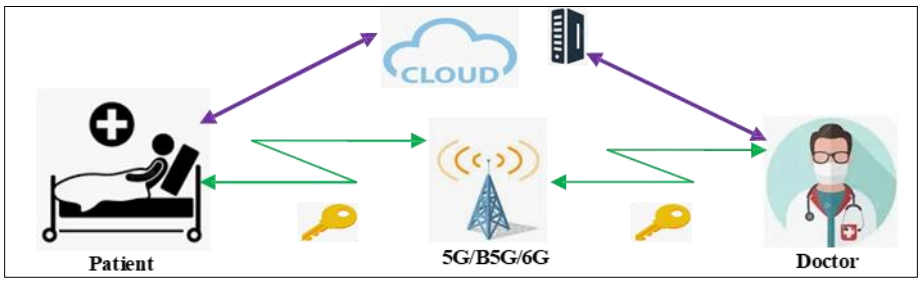

Figure 2 Proposed Secure IoMT Communication Architecture

- At the receiver end, all messages must be authenticated and when necessary, the source should be associated with this message.
- All diagnostic information in storage should not be lost or accessed by an adversary.
- The processing at the terminals should be quick enough so as to facilitate real-time response. This will also go a long way in preventing denial of service attacks.
- The power consumption on the sensors should be kept at minimum so as to conserve their battery power.

Based on these security and performance requirements, the following future research directions are formulated.

5. Future Research directions

Many security, privacy and performance challenges have been noted in the current IoMT communication environment. Although many schemes have been presented to address these issues, the attainment of perfect security at optimum performance remains a mirage. In this regard, the following technologies are thought to be essential towards the attainment of enhanced performance, security and privacy in IoMT applications.

5.1. Artificial Intelligent (AI)

Artificial intelligence deployment in IoMT will be critical for attack prediction and detection. In this way, any changes in the encryption key or the key size as well as the changes in the deployed encryption algorithm or scheme can be detected. This will facilitate the initialization of the necessary corrective measures for increased security and privacy preservation. Another possible area for AI deployment is network optimization [94]-[96]. For instance, the demand for short response times in real-time services is the most challenging aspect in IoMT. Here, machine learning algorithms can be applied for handoff optimization as well as target cell selection to minimize handover latencies [97]-[106]. In this way, the quality of service (QoS) of the offered remote access services will be enhanced. It is also possible to deploy AI technologies to prevent zero-day attacks as well as the identification of anomalous patent behavior using user or patient profiles.

5.2. Cloud Computing

In IoMT communication scenario, there are numerous data shared across the network participants. In this environment, cloud services are required for data storage and analytics. For instance, cloud computing services with high processing capabilities can be utilized to offload computationally intensive AI, machine learning, and deep learning processing from the sensor devices. This high power analytics can then provide quick predictions of critical cases of all threats and attacks. Although cloud computing provides scalability and wide deployments of IoMT systems, it imposes new security and privacy challenges. These challenges are reflected in data storage, transmission and processing in the cloud. There is therefore a need for more robust security protocols to protect the healthcare data residing in the cloud.

5.3. B5G and 6G Networks

The beyond 5G (B5G) and the Sixth Generation (6G) networks are the backbone of future IoMT deployments. Using these cellular technologies, high levels of performance and security can be attained. For instance, fast response times, high data rates up to 10 Gbps with low latency, high flexibility, high scalability, connectivity to heterogeneous devices, a wide range of supported applications as well as enhanced QoS are some of the goals pursued by these technologies [107]-[109]. However, attacks such as de-synchronization still presents some challenges in these networks. There is therefore need to come up with innovative schemes and protocols for eliminating these attacks.

6. Conclusion

Most of the challenges in IoMT revolve around privacy, performance, security, data integrity and authentication of critical healthcare data. Although these issues have attracted a lot of attention from the industry as well as academia, many gaps are still evident. These gaps are reflected in the observed privacy and security holes, as well as performance constraints. For instance, current technologies such as bilinear pairings, public key infrastructure, RSA, blockchain and elliptic curve point multiplication have been observed to have extremely high computation or communication overheads. On the other hand, identity-based schemes have been noted to have key escrow problems while trusted authority protocols presents some single point of failure. Output instability has been noted to be a key challenge in physically unclonable function based techniques, while password-based protocols are susceptible to dictionary, offline password guessing and brute forcing attacks. In summary, the attainment of perfect security at optimal performance still presents some challenges. To address some of these security and performance shortcomings, a scheme based on lightweight cryptographic operations is proposed. For performance enhancement, the proposed scheme uses 5G, B5G

or 6G as the backbone. Future work lies in the actualization of this scheme so that its security features can be analyzed against conventional IoMT attack vectors.

Compliance with ethical standards

Acknowledgments

The authors would wish to acknowledge the university college and colleagues who offered us moral support that enabled the timely completion of this work.

Disclosure of conflict of interest

The authors declare that they do not have any conflict of interest.

References

[1] Dewangan K, Mishra M, Dewangan NK. A review: A new authentication protocol for real-time healthcare monitoring system. Irish Journal of Medical Science (1971-). 2021 Aug; 190(3):927-32.

[2] Shariq, M., Singh, K., Bajuri, M. Y., Pantelous, A. A., Ahmadian, A., & Salimi, M. (2021). A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario. Sustainable Cities and Society, 75, 103354.

[3] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[4] Shariq M, Singh K. A novel vector-space-based lightweight privacy-preserving rfid authentication protocol for iot environment. The Journal of supercomputing. 2021 Aug; 77(8):8532-62.

[5] Guo C, Tian P, Choo KK. Enabling privacy-assured fog-based data aggregation in E-healthcare systems. IEEE Transactions on Industrial Informatics. 2020 May 19; 17 (3):1948-57.

[6] Xie S, Zhang F, Cheng R. Security enhanced RFID authentication protocols for healthcare environment. Wireless Personal Communications. 2021 Mar; 117(1):71-86.

[7] Butt SA, Jamal T, Azad MA, Ali A, Safa NS. A multivariant secure framework for smart mobile health application. Transactions on Emerging Telecommunications Technologies. 2019 Aug 6:e3684.

[8] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference 2022 (pp. 325-340). Springer, Cham.

[9] Soderi S, Mucchi L, Hämäläinen M, Piva A, Iinatti J. Physical layer security based on spread-spectrum watermarking and jamming receiver. Transactions on Emerging Telecommunications Technologies. 2017 Jul; 28(7):e3142.

[10] Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. Future generation computer systems. 2018 Jan 1; 78:956-63.

[11] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1; 11(1):185-94.

[12] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Jun 25:100210.

[13] Fotouhi M, Bayat M, Das AK, Far HA, Pournaghi SM, Doostari MA. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks. 2020 Aug 4; 177:107333.

[14] Habibzadeh H, Dinesh K, Shishvan OR, Boggio-Dandry A, Sharma G, Soyata T. A survey of healthcare Internet of Things (HIoT): A clinical perspective. IEEE Internet of Things Journal. 2019 Oct 9; 7(1):53-71.

[15] Srivastava K, Awasthi AK, Kaul SD, Mittal RC. A hash based mutual RFID tag authentication protocol in telecare medicine information system. Journal of medical systems. 2015 Jan; 39(1):1-5.

[16] Li CT, Weng CY, Lee CC. A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. Journal of medical systems. 2015 Aug; 39(8):1-8.

[17] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In 2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[18] Jin C, Xu C, Zhang X, Li F. A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety. Journal of medical systems. 2016 Jan; 40(1):1-6.

[19] prakash Pokala J, Reddy MC, Bapana S, Vorugunti CS. A secure RFID protocol for telecare medicine information systems using ECC. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) 2016 Mar 23 (pp. 2295-2300). IEEE.

[20] Kumar P, Lee SG, Lee HJ. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors. 2012 Feb 7; 12(2):1625-47.

[21] Noori D, Shakeri H, Niazi Torshiz M. Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment. EURASIP Journal on Information Security. 2020 Dec; 2020(1):1-1.

[22] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6:e4528.

[23] Zhou Z, Wang P, Li Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. Journal of ambient intelligence and humanized computing. 2019 Sep; 10(9):3603-15.

[24] Agrahari AK, Varma S. A provably secure RFID authentication protocol based on ECQV for the medical internet of things. Peer-to-Peer Networking and Applications. 2021 May; 14(3):1277-89.

[25] Jin C, Xu C, Zhang X, Zhao J. A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. Journal of medical systems. 2015 Mar; 39(3):1-8.

[26] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. In International Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[27] Das ML. Two-factor user authentication in wireless sensor networks. IEEE transactions on wireless communications. 2009 Mar 16; 8(3):1086-90.

[28] Yang J, Park J, Lee H, Ren K, Kim K. Mutual authentication protocol for low-cost RFID. In Workshop on RFID and lightweight crypto 2005 (pp. 17-24). WRLC.

[29] Piramuthu S. RFID mutual authentication protocols. Decision Support Systems. 2011 Jan 1;50(2):387-93.

[30] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. 2021, 3(4): 43-50.

[31] Salem FM, Amin R. A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. Information sciences. 2020 Jul 1; 527:382-93.

[32] Shen H, Shen J, Khan MK, Lee JH. Efficient RFID authentication using elliptic curve cryptography for the internet of things. Wireless personal communications. 2017 Oct; 96(4):5253-66.

[33] Chen Y, Chou JS. ECC-based untraceable authentication for large-scale active-tag RFID systems. Electronic Commerce Research. 2015 Mar; 15(1):97-120.

[34] Afroz T, Bhuiyan MN, Uddin MN. A Secure Mutual Authentication Protocol for IoT using ID Verifier Based on ECC. In 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI) 2019 Dec 24 (pp. 1-6). IEEE.

[35] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[36] Jan SU, Qayum F. Mitigating the desynchronisation attack in multiserver environment. IET Communications. 2020 Aug; 14(13):2210-21.

[37] Fan K, Jiang W, Li H, Yang Y. Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics. 2018 Jan 18; 14(4):1656-65.

[38] Benssalah M, Djeddou M, Drouiche K. Security analysis and enhancement of the most recent RFID authentication protocol for telecare medicine information system. Wireless Personal Communications. 2017 Oct;96(4):6221-38.

[39] Chen X, Geng D, Zhai J, Liu W, Zhang H, Zhu T. Security analysis and enhancement of the most recent RFID protocol for telecare medicine information system. Wireless Personal Communications. 2020 Sep; 114(2):1371-87.

[40] Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security. 2018 Sep 1; 78:126-42.

[41] Nyangaresi VO, Abduljabbar ZA, Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. In Ad Hoc Networks and Tools for IT 2021 Dec 6 (pp. 188-204). Springer, Cham.

[42] Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. Future generation computer systems. 2018 Jan 1; 78:956-63.

[43] Chung Y, Choi S, Lee Y, Park N, Won D. An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks. Sensors. 2016 Oct 7; 16(10):1653.

[44] Nyangaresi VO, Rodrigues AJ, Abeka SO. Efficient group authentication protocol for secure 5G enabled vehicular communications. In 2020 16th International Computer Engineering Conference (ICENCO) 2020 Dec 29 (pp. 25-30). IEEE.

[45] Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V. Secure anonymous mutual authentication for star two-tier wireless body area networks. Computer methods and programs in biomedicine. 2016 Oct 1; 135:37-50.

[46] Wang C, Zhang Y. New authentication scheme for wireless body area networks using the bilinear pairing. Journal of medical systems. 2015 Nov; 39(11):1-8.

[47] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[48] Liao YP, Hsiao CM. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad hoc networks. 2014 Jul 1; 18:133-46.

[49] Zhao Z. A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. Journal of medical systems. 2014 May; 38(5):1-7.

[50] Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Transactions on parallel and distributed systems. 2013 May 23; 25(2):332-42.

[51] Chen BL, Kuo WC, Wuu LC. Robust smart-card-based remote user password authentication scheme. International Journal of Communication Systems. 2014 Feb; 27(2):377-89.

[52] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[53] Chou JS. An efficient mutual authentication RFID scheme based on elliptic curve cryptography. The Journal of supercomputing. 2014 Oct; 70(1):75-94.

[54] Agrahari AK, Varma S. Authentication in RFID scheme based on elliptic curve cryptography. In Safety, Security, and Reliability of Robotic Systems 2020 Dec 30 (pp. 217-230). CRC Press.

[55] Farash MS. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. The Journal of Supercomputing. 2014 Nov;70(2):987-1001.

[56] Nyangaresi VO, Rodrigues AJ, Taha NK. Mutual authentication protocol for secure VANET data exchanges. In International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2021 May 6 (pp. 58-76). Springer, Cham.

[57] Li Q, Cao G. Multicast authentication in the smart grid with one-time signature. IEEE Transactions on Smart Grid. 2011 May 27; 2(4):686-96.

[58] Alotaibi M. An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access. 2018 Nov 9; 6:70072-87.

[59] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014; 16(5):137-44.

[60] Jiang Q, Lian X, Yang C, Ma J, Tian Y, Yang Y. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. Journal of medical systems. 2016 Nov; 40(11):1-0.

[61] Kamil IA, Ogundoyin SO. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. Journal of information security and applications. 2019 Feb 1; 44:184-200.

[62] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[63] Shao J, Lin X, Lu R, Zuo C. A threshold anonymous authentication protocol for VANETs. IEEE Transactions on vehicular technology. 2015 Feb 24; 65(3):1711-20.

[64] He D, Kumar N, Khan MK, Wang L, Shen J. Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Systems Journal. 2016 Dec 28; 12(2):1621-31.

[65] Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. Journal of medical systems. 2014 Feb; 38(2):1-7.

[66] Haider Z, Jamal T, Asam M, Butt S, Ajaz A. Mitigation of wireless body area networks challenges using cooperation. International Journal of Security and Its Applications. 2020; 14(1):15-30.

[67] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[68] Alamr AA, Kausar F, Kim J, Seo C. A secure ECC-based RFID mutual authentication protocol for internet of things. The Journal of supercomputing. 2018 Sep; 74(9):4281-94.

[69] Naeem M, Chaudhry SA, Mahmood K, Karuppiah M, Kumari S. A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things. International Journal of Communication Systems. 2020 Sep 10; 33(13):e3906.

[70] Tu YJ, Kapoor G, Piramuthu S. Security of lightweight mutual authentication protocols. The Journal of supercomputing. 2021 May; 77(5):4565-81.

[71] Sun X, Men S, Zhao C, Zhou Z. A security authentication scheme in machine-to-machine home network service. Security and Communication Networks. 2015 Nov 10; 8(16):2678-86.

[72] Parah SA, Kaw JA, Bellavista P, Loan NA, Bhat GM, Muhammad K, de Albuquerque VH. Efficient security and authentication for edge-based internet of medical things. IEEE Internet of Things Journal. 2020 Nov 13; 8(21):15652-62.

[73] Karthikeyan S, Patan R, Balamurugan B. Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism. In Recent Trends in Communication, Computing, and Electronics 2019 (pp. 217-225). Springer, Singapore.

[74] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[75] Schmitt C, Noack M, Stiller B. TinyTO: Two-way authentication for constrained devices in the Internet of Things. InInternet of Things 2016 Jan 1 (pp. 239-258). Morgan Kaufmann.

[76] Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In 2014 IEEE Wireless Communications and Networking Conference (WCNC) 2014 Apr 6 (pp. 2728-2733). IEEE.

[77] Farash MS, Nawaz O, Mahmood K, Chaudhry SA, Khan MK. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. Journal of medical systems. 2016 Jul; 40(7):1-7.

[78] Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on industrial electronics. 2016 Jun 27; 63(11):7124-32.

[79] Nyangaresi VO. ECC based authentication scheme for smart homes. In 2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[80] Rehman ZU, Altaf S, Iqbal S. An efficient lightweight key agreement and authentication scheme for WBAN. IEEE Access. 2020 Sep 24; 8: 175385-97.

[81] Xiao L, Xie S, Han D, Liang W, Guo J, Chou WK. A lightweight authentication scheme for telecare medical information system. Connection science. 2021 Jul 3; 33(3):769-85.

[82] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[83] Lai C, Li H, Lu R, Shen XS. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Computer Networks. 2013 Dec 9; 57(17):3492-510.

[84] Lai C, Lu R, Zheng D, Li H, Shen XS. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. Computer Networks. 2016 Apr 22; 99:66-81.

[85] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[86] He D, Kumar N, Chilamkurti N, Lee JH. Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. Journal of medical systems. 2014 Oct; 38(10):1-6.

[87] Lee CI, Chien HY. An elliptic curve cryptography-based RFID authentication securing e-health system. International Journal of Distributed Sensor Networks. 2015 Dec 24; 11(12):642425.

[88] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones. 2022 Jun 22; 6(7):154.

[89] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[90] Zhou E, Sun H, Pi B, Sun J, Yamashita K, Nomura Y. Ledgerdata refiner: a powerful ledger data query platform for hyperledger fabric. In 2019 sixth international conference on Internet of Things: Systems, Management and Security (IOTSMS) 2019 Oct 22 (pp. 433-440). IEEE.

[91] Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks. 2013 Nov 1; 11(8):2710-23.

[92] Durairaj M, Muthuramalingam K. A new authentication scheme with elliptical curve cryptography for internet of things (IoT) environments. Int. J. Eng. Technol. 2018; 7(2.26):119-24.

[93] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abduljaleel IQ, Abood EW. Towards Security and Privacy Preservation in 5G Networks. In 2021 29th Telecommunications Forum (TELFOR) 2021 Nov 23 (pp. 1-4). IEEE.

[94] Feltrin M, Tomasin S. A machine-learning-based handover prediction for anticipatory techniques in wi-fi networks. In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN) 2018 Jul 3 (pp. 341-345). IEEE.

[95] Saeed M, Kamal H, El-Ghoneimy M. A new fuzzy logic technique for handover parameters optimization in LTE. In 2016 28th International Conference on Microelectronics (ICM) 2016 Dec 17 (pp. 53-56). IEEE.

[96] Chinchali S, Hu P, Chu T, Sharma M, Bansal M, Misra R, Pavone M, Katti S. Cellular network traffic scheduling with deep reinforcement learning. In Thirty-second AAAI conference on artificial intelligence 2018 Apr 25.

[97] Colin I, Thomas A, Draief M. Parallel contextual bandits in wireless handover optimization. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) 2018 Nov 17 (pp. 258-265). IEEE.

[98] Nyangaresi VO, Rodrigues AJ. Efficient handover protocol for 5G and beyond networks. Computers & Security. 2022 Feb 1; 113:102546.

[99] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[100] Cai X, Wu C, Sheng J, Zhang J, Wang Y. A parameter optimization method for LTE-R handover based on reinforcement learning. In 2020 International Wireless Communications and Mobile Computing (IWCMC) 2020 Jun 15 (pp. 1216-1221). IEEE.

[101]] Chiumento A, Bennis M, Desset C, der Perre LV, Pollin S. Adaptive CSI and feedback estimation in LTE and beyond: a Gaussian process regression approach. EURASIP Journal on Wireless Communications and Networking. 2015 Dec; 2015(1):1-4.

[102] Nyangaresi VO, Rodrigues AJ, Abeka SO. Machine Learning Protocol for Secure 5G Handovers. International Journal of Wireless Information Networks. 2022 Mar; 29(1):14-35.

[103] Ma B, Guo W, Zhang J. A survey of online data-driven proactive 5G network optimisation using machine learning. IEEE access. 2020 Feb 19; 8:35606-37.

[104] Ozturk M, Akram M, Hussain S, Imran MA. Novel QoS-aware proactive spectrum access techniques for cognitive radio using machine learning. IEEE Access. 2019 May 22; 7: 70811-27.

[105] Zhu A, Guo S, Liu B, Ma M, Yao J, Su X. Adaptive multiservice heterogeneous network selection scheme in mobile edge computing. IEEE Internet of Things Journal. 2019 Apr 19; 6(4):6862-75.

[106] Nyangaresi VO, Rodrigues AJ, Abeka SO. ANN-FL secure handover protocol for 5G and beyond networks. In International Conference on e-Infrastructure and e-Services for Developing Countries 2020 Dec 2 (pp. 99-118). Springer, Cham.

[107] Yajnanarayana V, Rydén H, Hévizi L. 5G handover using reinforcement learning. In 2020 IEEE 3rd 5G World Forum (5GWF) 2020 Sep 10 (pp. 349-354). IEEE.

[108] Li R, Zhao Z, Zhou X, Ding G, Chen Y, Wang Z, Zhang H. Intelligent 5G: When cellular networks meet artificial intelligence. IEEE Wireless communications. 2017 Mar 27; 24(5):175-83.

[109] Yao J, Zheng X, Xie R, Wu K. Cross-Technology Communication for Heterogeneous Wireless Devices through Symbol-Level Energy Modulation. IEEE Transactions on Mobile Computing. 2021 Mar 17.