Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Security and Privacy in IoT Healthcare System: A systematic review

Rana Fadhel Atiyah[a], Intisar Al-Mejibli[b]*

a *Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers & Informatics, Iraq, Baghdad, email: ms202010602@iips.icci.edu.iq*

b *Biomedical informatics college, University of Information Technology and Communications, Iraq, Baghdad, email:* dr.intisar.almejibli@gmail.com

ARTICLE INFO

Article history:
Received: 06 /02/2022
Rrevised form: 25 /02/2022
Accepted : 10 /03/2022
Available online: 13 /03/2022

Keywords:

Internet of things, Security, Privacy, Smart Healthcare system

ABSTRACT

As technology advances worldwide, several governments and health organizations develop or implement mobile health systems and applications to treat and monitor patients. Several health systems based on the Internet of Things (IoT) applications have been built to monitor patients remotely. Different mechanisms and techniques have been used in healthcare applications, such as centralized, decentralized, and hybrid. In addition, many communication technologies were used, such as Bluetooth, GPS, WiFi, and others. This systematic analysis discusses these aspects, focusing on user security, privacy, effective data extraction, and confidential handling. This review investigates all researches published between 2015 and 2021, where four databases (IEEE Xplore, ScienceDirect, Research Gate, and Springer) were considered. A detail of used exclusion criteria and selection procedure to assess the collected publications were presented. Only thirteen papers have matched the criteria thoroughly examined and included in this study. The findings are provided throughout the papers to highlight gaps and concerns in an IoT-based healthcare system that will be constructed to effectively decrease potential dangers during messaging while preserving total user privacy and security.

MSC.41A25; 41A35; 41A3

https://doi.org/10.29304/jqcm.2022.14.1.882

1. Introduction

The Internet of Things (IoT) is a rapidly expanding ecosystem that connects software, hardware, physical objects, and computing devices to interact, collect, and share data. The Internet of Things (IoT) provides a seamless platform for people to connect with various physical and virtual things, including personalized healthcare domains. Loss of access to medical services, a growing senior populace with chronic illnesses, and their need for remote monitoring, rising medical expenses, and telemedicine in developing countries all make the Internet of Things (IoT) a fascinating issue in healthcare. The Internet of Things (IoT) can minimize the pressure on sanitary systems while simultaneously providing personalized health services to improve people's quality of life. In the last few years, smart healthcare systems have contributed significantly to economic growth, and they are increasingly

∗Corresponding author: Rana Fadhel Atiyah

Email addresses: *ms202010602@iips.icci.edu.iq*

Communicated by: Dr. Rana Jumaa Surayh aljanabi

seen as an integral part of that growth. As smart healthcare systems become more prevalent, IoT applications such as smart medication, telemedicine, and remote monitoring of medical resources are becoming more commonplace, allowing for the development of a wide range of new applications. Patients' adherence to treatment and behavioral changes. Internet of Things (IoT) refers to medical equipment with sensors and connectivity in the healthcare sector [1]. Hospitals' workloads could be lowered by eliminating needless hospital visits thanks to IoT. The sharing of sensitive medical data among diverse medical sectors is made possible by the safe transmission of data provided by this system as well. The applications of the Internet of Things have improved people's lives. IoT security, privacy, and trust issues arise frequently. Recently, the researcher community has paid increasing attention to security, privacy, and trust [2]. Figure (1) shows the security issues in IoT. The data require be securing and safeguarding in storage and transfer to ensure the data's integrity, validity, and most crucially, authenticity. It also provides that data may only be read and edited by authorized individuals. Another fundamental goal to consider while constructing an intelligent healthcare system is privacy preservation (PP). When shared data is communicated across an open and insecure channel, it primarily accounts for the severity and sensitivity of the data. PP necessitates both content and context. Content privacy protects patient information against data leakage; however, protecting patients' privacy is challenging since an attacker can determine the health status based on the doctor's identity. The protection of contextual privacy is equally essential. A communication's context is protected by contextual privacy. Many symmetric and asymmetric encryption techniques are used in an IoT-enabled smart healthcare system to ensure patient privacy [3].

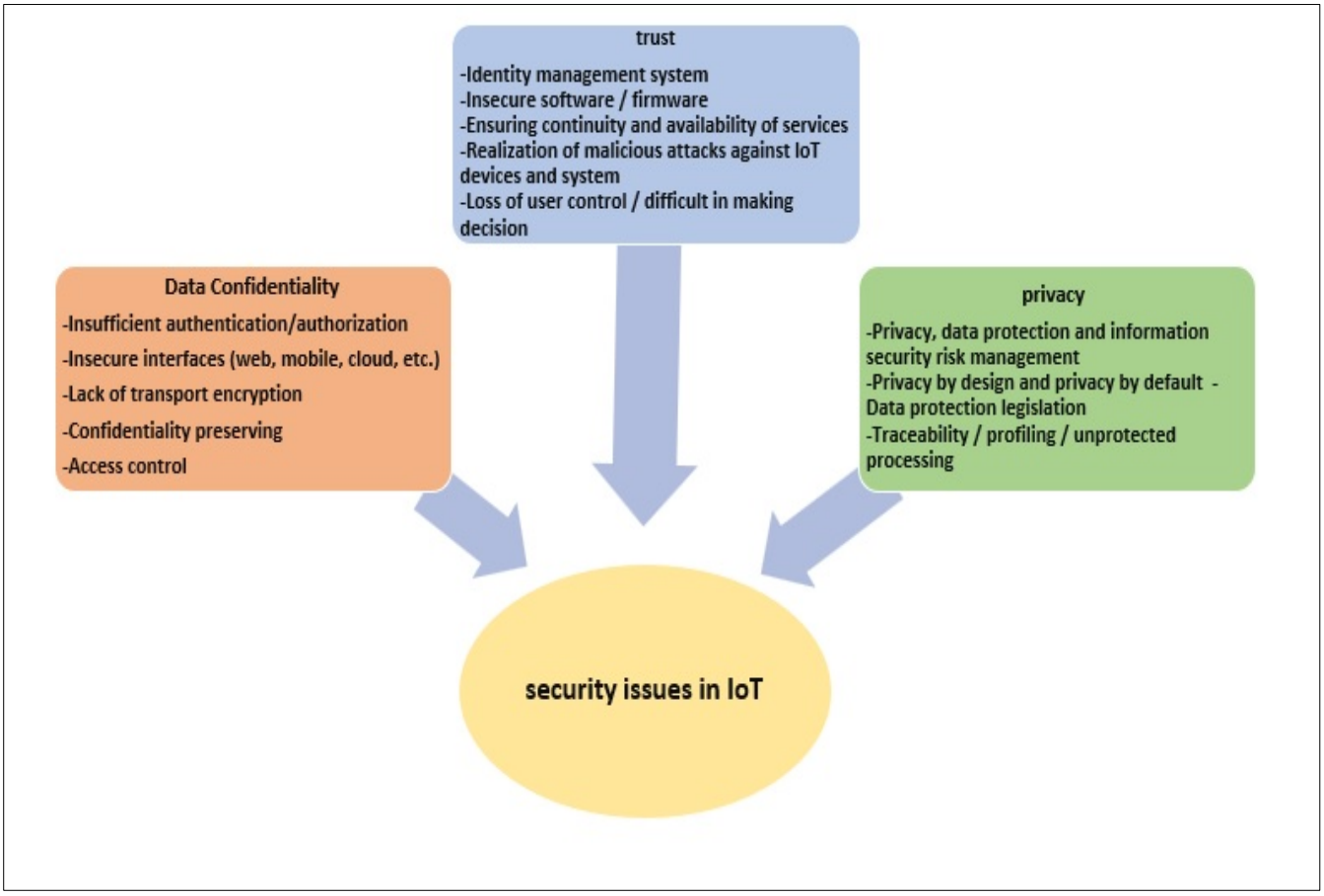

Figure (1). The security issues in IoT.

The literature has recently stated that using complex machine learning (ML) methods on resource-restricted devices like IoT is not the best approach [1]. However, it can be solved by implementing simple PP approaches on IoT devices and exploiting the cloud's advantages for complicated ML algorithms [4],[5]. Many studies based on cloud-related security solutions for IoT in smart healthcare systems have been published in the literature. This study seeks to provide an overview of several security, privacy, and trust strategies for IoT-enabled smart

healthcare systems that have been published in recent years. Finally, it finishes with a few suggestions for future study topics.

2. Method

We followed the suggested reporting elements for systematic reviews and meta-analyses [6]. The four numerical databases were IEEE Xplore, ScienceDirect (SD), ResearchGate (RG), and Springer. IEEE Xplore is a database of high-quality engineering and information technology books. SD is a highly respected journal that provides access to scientific, technological, and medical research. In engineering, social sciences, humanities, and interdisciplinary studies, RG is a highly regarded resource. In the technical, scientific, and medical publications, Springer hosts a number of scientific databases. The four databases provide an overview of the IoT and its applications, particularly the health care system. In addition, explore the methods of keeping patient information confidential and private while sending messages via the Internet from the patient's site to the health centers associated with them and vice versa. The findings of this literature study can be used to help create future applications and make them more convenient and acceptable to users, preventing any security breaches in the health system that affect patients data.

3. Search strategy

Based on the four aforementioned databases, we extensively reviewed the literature published in English between 2015 and 2021. Because the health care system via the (IoT) requires more attention than any other system, the criteria for selecting surveys indicate that they are eligible for inclusion in our study. For various keywords, this study described and implemented a Boolean search strategy (e.g., security, privacy, confidential, threats, IoT, Internet of Medical Things (IoMT), Smart healthcare). These query approaches boost research in numerous studies of smartphone platforms and contact tracking applications. The following are the requirements for inclusion:

1. A journal or conference article in English is used as the primary source.

2. The major objective is to improve healthcare apps, systems, and technology-based on the Internet of Things.
3. Improvement is primarily focused on protecting patient security, privacy and confidentiality.

4. Study selection

This approach began with removing duplicate papers and screening titles and abstracts for non-duplicated articles to ensure that they met our inclusion and exclusion criteria. The relevant publications were exposed to a comprehensive reading procedure to collect, extract research data and generate the review article. All research papers have been thoroughly read and studied to ensure the construction of a highly accurate and relevant systematic review in this research report.

5. Data Extraction and selection

Extraction of data and classification of selected studies, including data relating to the security and privacy of an Internet-of-Things-based health care system, in order to determine the utility of this system in terms of detecting, tracking, and notifying individuals who are close to or responsible for any threat or hack that results in harm to patients. The following data were extracted from the scientific literature: authors' nationalities, publication dates, number of publications each year, and number of articles in the database. To provide a thorough overview of the uses of the Internet of Things in healthcare, this study evaluated the system and analysed its global growth potential utilizing various frameworks and strategies for recording, communicating, and securing data. This analysis compiled a list of each method's distinguishing traits and characteristics for each literature search. The problems, constraints, and recommendations stated in this section were derived from the peer-reviewed studies in order to create a more adaptable, dependable, and transparent system.

6. Results

The results of the proposed query used in this study are shown in Figure (2). The first set of results included 600 papers from all four databases. There were 4 duplicated articles across all databases, with 596 results. The next step was to screen publications based on their title and abstract, then map the inclusion and exclusion criteria, resulting in 153 articles

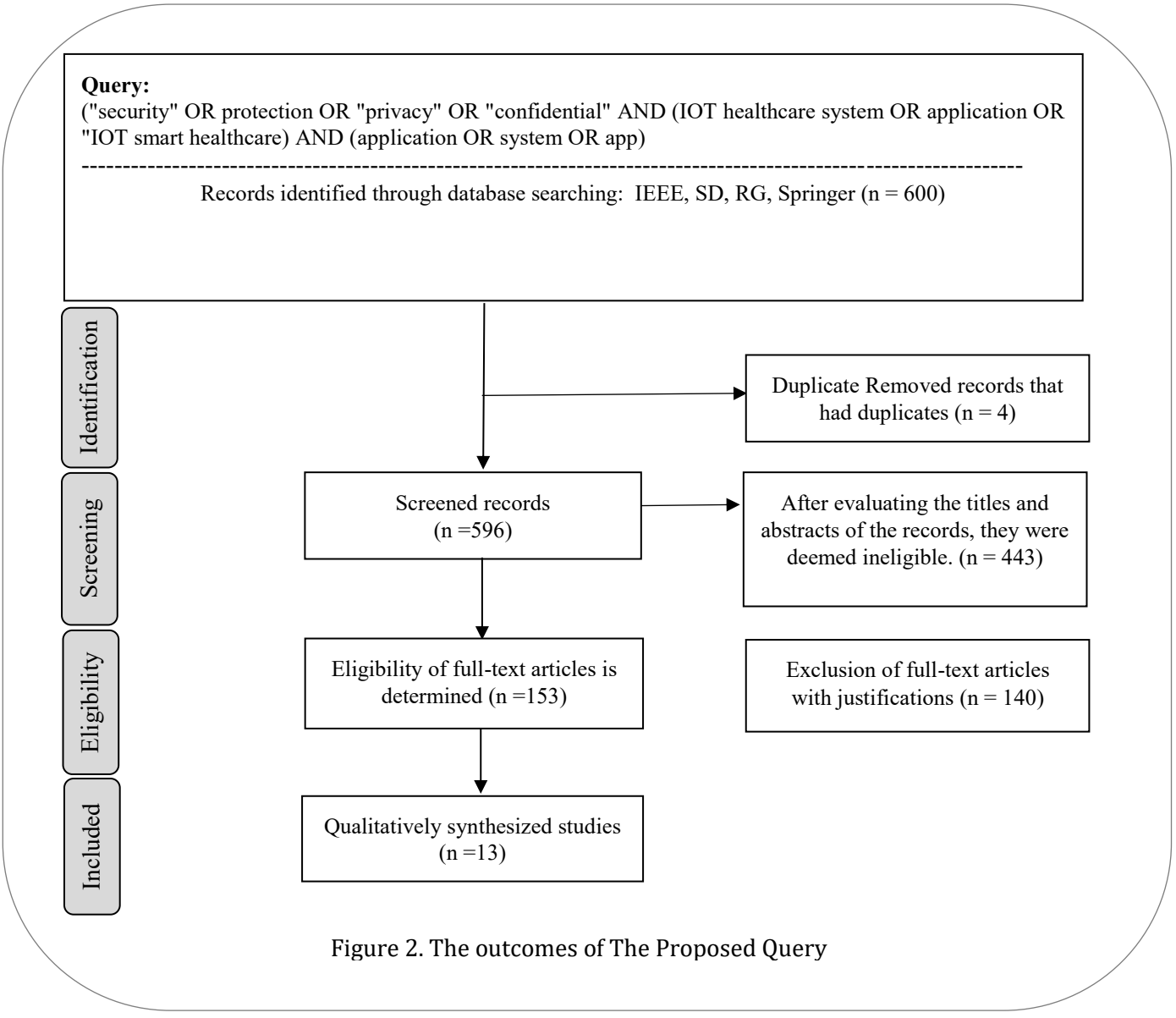

Figure 2. The outcomes of The Proposed Query

7. Discussion

By processing historical data and integrating various IoT devices to gather real-time physiological data from patients, such as blood glucose levels, temperature monitors, and other vital data, IoT has changed the sanitary system into a predictive and intelligent one. The principal purpose is to provide the patients with high-quality of medical services, such as early disease identification and continuous monitoring of dangerous diseases. Indeed, the Internet of Things may benefit the healthcare business in various ways, including preventative care, illness management, supported living, and remote clinical monitoring. In addition, some of the most frequent IoT applications in healthcare are in sectors, for instance, home healthcare, mobile healthcare or e-healthcare, and hospital administration [7][8].

Intelligent healthcare processes, self-care, and the detection of some events, such as seizures, falls to help Parkinson's gait disturbances and stroke rehabilitation, neurologic monitoring, and cardiac monitoring have been made possible thanks to the convergence of the Internet of Things (IoT) and healthcare systems. Healthcare apps must overcome many challenges, including self-improvement and self-learning as well as hardware systems (such as implantable sensors and wearables), privacy and security, as well as standards, to be prosperous and secure. Security protocols, including public-key cryptosystems, k-anonymity, and other mechanisms for data authentication and encryption, are already available [9][10]. We identified thirteen studies on security, privacy, and effective data extraction and confidential data handling in IoT healthcare systems with a summary of the characteristics, as shown in (Table1).

He and Zeadally (2015) offered a security and performance study of RFID authentication methods based on elliptic curve cryptography (ECC) and the security requirements for RFID authentication systems in the healthcare environment. As long as the proposed ECC-based RFID authentication technique maintains reasonable computational and communication costs, it satisfies all security requirements [11].

Yeh (2016) introduced two safe authentication systems based on body sensor networks for IoT-based healthcare (BSNs). The Raspberry PI platform was used to demonstrate the feasibility and practicability of the proposed strategies. Standard intelligent mobile devices with high-security density and secrecy can be implemented using the offered methods. SHA-2 attacks can be used against the proposed methods. [12].

Elhoseny et al. (2018) used hybrid AES and steganography encryption techniques to provide high dependability, capacity imperceptibility as well as low degradation in the transfer of medical data [13].

Nidhi and Ravindara (2018) suggested a privacy-preserving method based on multipath routing, secret sharing, and hashing for WSN-based healthcare applications[14]. S. Kavitha1(2019) The proposed framework addresses security problems by using a public-key cryptosystem based on hyper elliptic curves that combine Digital Signature and Elgamal techniques to ensure entity authentication and safe group communication. The suggested work's performance was evaluated using effective security mechanisms compared to similar schemes [15].

Rani et al. (2019) proposed an approach for securing healthcare data that uses the SIMON block cipher algorithm and a shared generation architecture to ensure the highest levels of security and privacy. Experiments demonstrated the scheme's efficiency and performance in energy cost, throughput, reaction time, execution time, and latency; nonetheless, the technique employed only specialized and limited algorithms [16].

Karthigaiveni and Indrani (2019), elliptic curve encryption, and a smart card were used to create a strong password with two-factor authentication for use in IoT healthcare. Random oracle model research showed that the method was safe and cost-effective, but privacy concerns were unaddressed [17]. Rathee et al., (2019) It has been possible, through blockchain, to create a safe framework for storing health multimedia data and to create a hash of each record. Therefore, any modification in data was copied across the whole blockchain network, making unlawful conduct impossible [18]. "Abou-Nassar et al. (2020)" has proposed a blockchain-based distributed trust system for safeguarding patient data and enhancing HIoT access control, interoperability, and security [19]. "Sahoo et al. (2020)" ECC was employed, and a key agreement and three-factor authentication mechanism were demonstrated. It offers security, mutual authentication, and user anonymity while requiring little computational and communication resources [20].

"Fotouhi et al. (2020)" suggested a hash chain-based authentication technique for WBANs in HIoT that ensures security and authenticity while using little computational and storage resources. It is proposed that the scheme be broken down into four stages: initialization; registration; authentication; and the changing of 175 passwords. Messages sent during the registration step are transmitted over a safe and private channel, whereas messages sent during the authentication and password change stages are sent over an insecure public channel. [21]. "

Islam and Young Shin (2020)" presented a blockchain-based secure healthcare design with security features. The proposed scheme is implemented on a variety of hardware in order to determine the impact of the security mechanism on real-world hardware performance. [22].

Ming et al. (2020) an efficient sign cryption technique based on certification was suggested, which guarantees anonymity, confidentiality, privacy, and unforgeability by combining certificate-based encryption and "ECC" [23]. The goal of this study was to emphasize the academic literature's recommendations for remedies to some of the difficulties.

Table 1. Summary of the Literature Researches Characteristics

Authors	Encryption technique	Used hashing	pros	cons
He and Zeadally (2015) [11]	(ECC)-based RFID	No	➢High confidentiality ➢High availability ➢High security ➢High scalability ➢Low cost ➢Low overhead	➢Vulnerable to some attacks
Yeh (2016) [12]	SHA-2 techniques	crypto-hash-modules	➢High efficiency ➢High confidentiality	➢Vulnerable to SHA-2 or 3 attacks ➢High overhead
Elhoseny et al., (2018) [13]	AES, steganography, and RSA encryption algorithms	NO	➢High security ➢High optimization ➢High stability ➢High performance	➢low scalability (used only AES and RSA)
Nidhi and Ravindara (2018) [14]	multipath routing, and secret sharing	hashing	➢High security ➢High privacy ➢better performance	➢High-cost ➢High latency
S. Kavitha1(2019) [15]	hyper elliptic curves that combine Digital Signature and Elgamal techniques	No	➢better level of security ➢high privacy	➢Vulnerable to some attacks
Rani et al., (2019) [16]	SIMON block cipher algorithm	NO	➢High security ➢High privacy ➢High optimization ➢Low latency ➢Low energy	➢Low scalability
Karthigaiveni and Indrani (2019) [17]	elliptic curve cryptography and a smart card	No	➢High security ➢Low latency ➢Low overhead	➢Low privacy ➢Low scalability
Rathee et al., (2019) [18]	blockchain	No	➢High security ➢High accuracy ➢High reliability	➢High-cost ➢High latency
Abou-Nassar et al., (2020) [19]	blockchain	No	➢High security ➢High privacy ➢High confidentiality ➢High interoperability ➢High integrity ➢High scalability ➢High availability ➢High trustworthy	➢Low diagnosis accuracy ➢High-cost ➢High latency
Sahoo et al., (2020) [20]	ECC	No	➢High security ➢Low cost ➢Mutual authentication ➢User anonymity	➢Without considering nonrepudiation, unlinkability, and untraceability

Table 1. (continued)

Authors	Encryption technique	Used hashing	pros	cons
Fotouhi et al., (2020) [21]	authentication technique for WBANs	hash chain	➢High security ➢High untraceability ➢High efficiency ➢Low cost ➢Low storage ➢Sensor anonymity	➢Low scalability
Islam and Young Shin, (2020) [22]	blockchain	No	➢High security ➢Low energy	➢Low-performance ➢High latency ➢High cost
Ming et al. (2020) [23]	certificate-based encryption and ECC	No	➢High security ➢High privacy ➢High confidentiality ➢Unforgeability ➢Anonymity ➢Low computation ➢Low communication cost	➢ Low scalability

8. Challenge and Limitation

Many factors must be considered by any MIoT security and a private developer to reach a better equilibrium. In order to strengthen the security environment, several issues must be addressed, including network channel issues. Unauthorized access to routers, man-in-the-middle attacks, spoofing, denial-of-service attacks, brute-force assaults, and traffic injections are only a few of the known vulnerabilities of wireless networks like WiFi [24]. Furthermore, the majority of public wireless networks that aren't certified are unreliable [25]. Data privacy, confidentiality, access control, and the financial motive for patient information are only a few of the many ethical issues that obstruct data exchange between patients and healthcare facilities. As a result, getting a complete picture of a patient's data becomes difficult [26].

9. Conclusion

Today, technology is transforming our lives and propelling us into a more technologically advanced world. Researchers worldwide are finding new ways to integrate IoT with various healthcare solutions to improve the existing healthcare infrastructure alleviate the strain caused by a lack of medical staff facilities and the aging population, chronic diseases, and global pandemics. Achieving this integration successfully requires maintaining the security, privacy, and confidentially of health information during transmission and storage. The investigated studies show that all of them implemented different security techniques, whereas only three researchers used hashing function to keep privacy. This article examines various facets of the IoT in healthcare; despite of there are three researches use blockchain technology that use hashing technique but that is more difficult to scale because of their consensus approach, as they are a sluggish process that can slow down when there are too many users on the network, and it required high energy consumption. Where specific solutions take too much energy, data immutability, where data cannot be changed, inefficiency due to how they operate, and still not mature. Five of the investigated researches used the ECC technique where it is difficult to put in place firmly since it is so complicated. The standards aren't cutting-edge. Theoretically, newer algorithms could contain undisclosed flaws. It might be pricey with ECC; public key operations (such as signature verification rather than a signature generation) are slow and, in some cases, have low scalability. Only one research used SAH-2 techniques, but it is vulnerable to SHA-2 or 3 attacks, while the studies used AES and RSA where RAS technology necessitates much energy. RAS also require a continuous power source. The installation process is relatively complicated, and it necessitates a high level of safety; with an unnecessarily simplistic algebraic structure that encrypts all blocks in exactly the same way, it has very

limited scalability. In addition, it isn't easy to implement through software. Finally, software implementation of AES in counter mode is problematic from performance and security perspectives. A set of proposals has been developed to address many issues, including maintaining the privacy and restricting access to data, while also considering the most significant issue, which is the heterogeneity of devices and their specific resources. In addition to ensuring that these tools are scientifically and ethically sound to ensure public trust and widespread use. The purpose is to perform new research that will aid governments and health institutions in their usage of cutting-edge technology by utilizing the characteristics and features gathered in the literature.

References

[1] K. K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, and C. Thapa, "Towards a security-enhanced virtualised network infrastructure for the internet of medical things (iomt)," in 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 257–261, IEEE, 2020.

[2] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," Wireless Networks, pp. 1–7, 2020

[3] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in 2019 15th international conference on distributed computing in sensor systems (DCOSS), pp. 457–464, IEEE, 2019.

[4] B. A. Alqaralleh, S. N. Mohanty, D. Gupta, A. Khanna, K. Shankar, and T. Vaiyapuri, "Reliable multi-object tracking model using deep learning and energy-efficient wireless multimedia sensor networks," IEEE Access, vol. 8, pp. 213426–213436, 2020.

[5] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing," Wireless Personal Communications, pp. 1–24, 2021.

[6] Moher, D., Liberati, A., Tetzlaff, J. & Altman, D. G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med. 6, e1000097 (2009).

[7] Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., Alizadeh, M., 2018. The application of Internet of things in healthcare: a systematic literature review and classification. Univers. Access Inf. Soc. 18 (4), 837–869.

[8] Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A.S., Satapathy, S.C., 2018. Internet of Things and Big Data Analytics toward Next-Generation Intelligence. Springer.

[9] Wilson, D., 2017. An overview of the application of wearable technology to nursing practice. Nursing Forum, 52. Wiley Online Library, pp. 124–132, 2.

[10] Ahmed, A., Latif, R., Latif, S., Abbas, H., Khan, F.A., 2018. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. Multimed. Tool. Appl. 77 (17), 21947–21965.

[11] He, D., Zeadally, S., 2015. An analysis of RFID authentication schemes for the Internet of things in a healthcare environment using elliptic curve cryptography. IEEE Internet of things journal 2 (1), 72–83.

[12] Yeh, K.-H., 2016. A secure IoT-based healthcare system with body sensor networks. IEEE Access 4, 10288–10299.

[13] Elhoseny, M., Ramírez-Gonz´alez, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A., 2018. Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6, 20596–20608.

[14] Sharma, N., Bhatt, R., 2018. Privacy Preservation in WSN for Healthcare Application. International Conference on Computational Intelligence and Data Science. Procedia Computer Science 132 (2018) 1243–1252.

[15] S. Kavitha & P. J. A. Alphonse & Y. Venkataramana Reddy, An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System. Journal of Medical Systems (2019) 43:260.

[16] Rani, S.S., Alzubi, J.A., Lakshmanaprabu, S., Gupta, D., Manikandan, R., 2019. Optimal users based secure data transmission on the Internet of healthcare things (IoHT) with lightweight block ciphers. Multimed. Tool. Appl. 78 (9), 35405–35424.

[17] Karthigaiveni, M., Indrani, B., 2019. An efficient two-factor authentication scheme with the key agreement for IoT-based E-health care application using a smart card. Journal of Ambient Intelligence and Humanized Computing 10 (10), 1–12.

[18] Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R., 2019. A hybrid framework for multimedia data processing in IoT healthcare using blockchain technology. Multimed. Tool. Appl. 79 (11), 9711–9733.

[19] Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O., Bashir, A.K., El-Latif, A.A. A., 2020. DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8, 111223–111238.

[20] Sahoo, S.S., Mohanty, S., Majhi, B., 2020. A secure three-factor-based authentication scheme for health care systems using IoT-enabled devices. Journal of Ambient Intelligence and Humanized Computing 12 (1), 1419–1434.

[21] Fotouhi, M., Bayat, M., Das, A.K., Far, H.A.N., Pournaghi, S.M., Doostari, M.A., 2020., healthcare applications and issues. Int. J. Inf. Manag. 33 (5), 875–891., A lightweight and secure two-factor authentication scheme for wireless body area networks in healthcare IoT. Comput. Network. 177, 107333–107350.

[22] Islam, A., Young Shin, S., 2020. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicles in the Internet of Things. Comput. Electr. Eng. 84, 106627–106642.

[23] Ming, Y., Yu, X., Shen, X., 2020. Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare internet of things. IEEE Access 8, 153561–153576.

[24] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "PPM-HDA: privacy-preserving and multifunctional health data aggregation with fault tolerance," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940–1955, 2016.

[25] H. Zhang, Z. Cai, Q. Liu, et al., "A survey on security-aware measurement in SDN," Security and Communication Network, vol. 2018, Article ID 2459154, 2018.

[26] BK. Rai, A. Srivastava, Security and privacy issues in healthcare information system, Int. J. Emerg. Trends Technol. Comput. Sci. 3 (6) (2014).

[*27] Mahawash Al-Jubouri, A. and Surayh Al-Janabi, D.R. 2021. SECURE RSA CRYPTOSYSTEM BASED ON MULTIPLE KEYS. Journal of Al-Qadisiyah for computer science and mathematics. 13, 3 (Aug. 2021), Comp Page 25 -33, . DOI:https://doi.org/10.29304/jqcm.2021.13.3.824.*

[28] Jarah, N. (2021). Deep Learning In Wireless Sensor Network. Journal of Al-Qadisiyah for Computer Science and Mathematics, 13(1), Comp Page 11 -17. https://doi.org/10.29304/jqcm.2021.13.1.755.

[29] Sabeeh Mahmood, G., Mohammed Hasan, T., & Mudheher Badr, A. (2017). Multi-Authority System based Personal Health Record in Cloud Computing. Journal of Al-Qadisiyah for Computer Science and Mathematics, 9(1), 108-116. Retrieved from https://qu.edu.iq/journalcm/index.php/journalcm/article/view/20.