pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220970

An Overview on Security and Privacy of Data in IoMT Devices: Performance Metrics, Merits, Demerits, and Challenges

Pankaj KHATIWADA[1] and Bian YANG
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. The Internet of Medical Things (IoMT) emerges with new trendsetter device applications, where it defines the incorporation of medical devices with the Internet of Things (IoT). The healthcare sector continues to encounter challenging obstacles that have an impact on the quality of treatment provided to patients. To get rid of this problem, IoMT is being deployed to achieve the high reliability and efficiency of the health system. The IoMT devices are superimposed with clinical information as they contain the details of patient health data, address, and other patient identifiers. By containing such amount of sensitive information, it becomes cumbersome to preserve data privacy and security. Due to inadequate security and privacy precautions, patient health data is susceptible to leakage, which has a direct impact on the patient's life. In addition, the majority of medical devices are susceptible to cyberattacks, putting patient information at risk. Inadequate control of life-support equipment can have a devastating effect on patient outcomes. Thus, this survey intends to review the various security models of IoMT devices using standard techniques to support health care systems. It provides a wide range of literature reviews regarding IoMT systems and compares them with traditional methodologies. This review work exhibits the motivation for current technologies to maintain the security and privacy of patients' data with IoMT devices. The systematic review entails background on security in IoMT devices, techniques for security, usage of diverse validation measures, and also discusses the problems and motivation for future research work.

Keywords. Internet of Medical Things; Security and Privacy of Data; Encryption; Blockchain; Authentication; Performance metrics

Introduction

Nowadays, IoMT has become the emerging technology to manage the patient's health information [1]. It is mainly used for various applications in hospitals, body sensors and homes. The IoMT environment is built with the collection of enormous medical devices, sensors and so on [2]. These efficient devices also have the potential to wear over the individual body surface. Due to the rapid development of the IoMT system, the medical industry can easily handle the medical information [3], where the practitioner aids in early detection of disorders and diagnosing effectively.

[1] Corresponding Author. Pankaj Khatiwada, Dept. of Inf. Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway; Email: pankaj.khatiwada@ntnu.no

Though the evolutionary growth of IoMT applications is observed in recent years [4], it confines with the two concerns as privacy and security. Over the IoMT infrastructure, it is critical to administer the health data as it contains myriads medical data [5]. Owing to the illustration of IoMT network, several attacks can be easily intruded and degrades the performance. Thus, it fails to preserve the significant data [6]. The system becomes vulnerable with respect to inadequate authorization or authentication of medical devices or sensors, lack of knowledge [7] about encrypting the data, insecurity of device interface, etc. The foremost technique to build the effective [8] IoMT system is authentication mechanisms to secure and privacy preserve the patient's data. Also, encryption techniques like Elliptic Curve Cryptography (ECC), Diffie-Hellman technique, etc. are employed to generate the cipher [9] text data that defends from malicious threats. Over the recent years, blockchain technology [10] has been immensely involved in the IoMT applications, where it enhances the security performance. However, all the aforementioned techniques restricts with few shortcomings [11] to protect the medical information. The main contribution of survey is as follows as (i) to demonstrate the various methodologies used for secure and privacy preserve of data in IoMT that belongs to recent developed paper, (ii) to categorize the algorithms used for IoMT application with its future scope and (iii) to discuss the chronological analysis for IoMT devices and its performance measures used for validation and (iv) to provide the research gaps and challenges for secure and privacy of data in IoMT devices.

The remaining section of the paper is follows. Section II explores the existing works based on 20 reference papers and its chronological review. Section III provides the basic introduction of IoMT along with performance measures. The merits, demerits, research gaps and future challenges are discussed in Section IV. Section V brings the closure of survey paper.

1. Literature Review

1.1. Related Works

Kumar and Tripathi [12] have proposed the consortium based blockchain network in terms of smart contracts for preserving the data in IoMT platform. It has integrated with the Inter Planetary File Systems (IPFS) cluster node, in which the authentication was needed to access the patient's clinical data by smart contracts. Furthermore, the cluster layer was also used for storage purpose. After authentication, the data was securely transmitted with the aid of consortium blocks. On the contrary of other implemented works, the suggested method has illustrated that it has achieved higher security level. Ogundokun et al. [13] have explored the concept of Crypto-Stegano method for securing the medical information over the IoMT infrastructure. This model was developed by inferring the methodologies of both cryptography and steganography. Finally, the valid information was acquired, which was used to evaluate the performance. Thus, the outcome has ensured that it has delivered better effective results in terms of data loss, security and capability and perceptible quality, thereby, it has proved an efficient model. Mohan et al. [11] have developed the private blockchain technique to maintain medical information securely. It has created a decentralized network, where the data was to be stored significantly. Here, in order to provide the data confidentiality, the Elliptic Curve Integrated Encryption Scheme was employed to do double encryption process. Thus, the performance was assessed, and it has achieved as less transaction time, thus, it has

obtained the more security for privacy preserving the data. Abbas et al. [14] have investigated the novel approach of Blockchain-assisted Secure Data Management Framework (BSDMF) in IoMT platform. It has performed the secure data management that was happened among the personal and cloud servers as well as utilized medical equipment's and personal servers. In addition to this, the blockchain model was taken for guaranteeing the data transmission over IoMT environment. Finally, the experimentation was carried out, and its results were validated using different measures as more accuracy and precision rate and trust factor and also reduced the response time. Wang et al. [15] have described the "Efficient Privacy preserving outsourced Support Vector Machine (EPoSVM)" for IoMT sector. In order to securely train the SVM network, it has deployed eight various secure-based computation protocols. Therefore, the trained data was obtained as secure manner and it has proved the privacy of the medical information while testing the model. Hence, the evaluation was elucidated that the recommended method has achieved the high security and privacy rather than former approaches. In 2021, Sun et al. [16] have presented the hybrid model for securing and preserving the data over IoMT. Here, the novel hybrid model was developed by the combination of both "Medium Access Control (MAC) and Enhanced On-Demand Vector (EAODV)-enabled routing". Initially, the registration process was carried out for devices in the offline phase. Therefore, it has blocked the illegitimate devices into the network. After this process, when the device has initiated the process, its corresponding server has to send the mutual authentication procedure. Over the sessions, the data integrity and reliability were maintained by influencing the encryption and decryption process. Finally, the simulation results have declared that it has enhanced the efficiency.

Egala et al. [17] have proposed the hybrid technique of preserving the data in IoMT platform, named as blockchain-based Distributed Data Storage System (DDSS). It has the main objective of diminishing certain constraints with the parameters like latency and storage cost. In order to perform a better authentication of entering the device into the network, the Selective Ring based Access Control (SRAC) was utilized. Finally, the performance was measured and thus it has obtained the impressive results to deliver the effective process of preserving the data. In 2021, Aslam et al. [18] have utilized the ANFIS model in the manner of blockchain based security management for IoMT applications. The main aim of this model was to aid the individuals to do the daily activities and also protect from the infected person. Here, the K-Nearest Neighbor (KNN) was also employed to analyze the performance in terms of accuracy measure. Li *et al.* [19] have presented the novel framework of Mutual Authentication and Key Agreement (MAAKA) by the characteristics of Provably-Secure and Lightweight (PSL), named as PSL-MAAKA for IoMT. The authentication process was carried out that has assisted by XOR and Hash operations, correspondingly. Furthermore, a security analysis was made through the concept of random oracle model. Finally, the experimental results have elucidated that the proposed scheme has obtained less overhead complexity. Ding et al. [20] have introduced the Deep learning approach of Encryption and Decryption Network (DeepEDN) for securing medical information. Here, it has taken the medical images for experimentation. In order to learn the image related data, Cycle-Generative Adversarial Network (Cycle-GAN) has been deployed. Further, the "Hidden Factors" of the learning technique were used to do the encryption phase, which could be restored while doing the decryption. Finally, the performance was validated, and its respective outcome has ensured to improve the system efficiency and better performance. Guan *et al.* [21] have enhanced the model of Efficient Differentially Private Data Clustering scheme (EDPDCS). Here, the K-Means clustering was employed to choose the initial centroid

data point and optimized the allocation of budget for increasing the accuracy. Over the iteration, the minimum and fixed value were considered for privacy budget. Owing to the clustering approach, the efficiency and accuracy were improved. Finally, the performance was analyzed and proved that it has acquired the better data preserving performance. Saba *et al.* [22] have framed a secure and efficient network over IoMT platform. The prime intention of this work was to mitigate and evade the overhead problem among the biosensors that it has employed. It has also required to secure the patient's medical data. Hence, the enhanced mechanism has appropriately ensured the integrity of the network, energy consumption of biosensors, less delay and low packet loss ratio.

Sowjanya et al. [23] have explored the lightweight authentication based Elliptic Curve Cryptography for IoMT platform. It was implemented in AVISPA tool and standard protocols were utilized to secure the medical information. Hence, the formal and informal way of approach was employed for security performance analysis. Comparative analysis was made to ensure the proposed scheme has increased the robust efficiency of IoMT devices. Alsubaei et al. [24] have recommended the ontology-oriented IoMT Security Assessment Framework (IoMT-SAF) for IoMT sector. Based on the customer prerequisite, it has identified the best solutions that were aided to make the better decision for securing the information. Finally, it has outperformed with its performance improvement. Chen et al. [25] have framed the asymmetric based encryption and authentication process over the IoMT environment. Here, the transmission mechanism has also involved for storage purpose, which was governed by distributed symmetric encryption. Along with this, authentication and authorization were carried out. Hence, the extensive outcome has demonstrated that it has acquired desired performance. Aghili et al. [26] have presented the novel lightweight authentication process for securing the medical information. Here, the proposed framework was termed as Lightweight Authentication, Access Control and Ownership (LACO). The major concern was considering the ownership transfer, where the server could modify the patient clinical data. Further, LACO mechanism was introduced against such attacks like insider attacks and Denial of Service (DoS). Hence, the performance results were validated and measured. Yi and Nie [27] have demonstrated the Multivariate-Quadratic-Equations (MQ) public-key cryptography and rainbow model of cryptographic scheme for IoMT applications. This algorithm was employed for end-to-end service that has resisted to such threats. Hence, certain countermeasures were considered to evaluate the performance. Thus, outstanding results were acquired to provide the better performance. Rani *et al.* [28] have influenced the Hybrid Teaching and Learning Based Optimization (HTLBO) for rendering the optimal results. Here, the Chinese Remainder Theorem (CRT) was developed to determine the security and authentication process. Finally, the extensive results have revealed that it has achieved less energy cost and computation time. Garg *et al.* [29] have suggested the "Blockchain Enabled Authenticated Key Management Protocol for IoMT (BAKMP-IoMT)" for managing the medical data securely. It was implemented in Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, where it has significantly resisted to several attacks. Finally, the simulation was performed and its results were validated via diverse measures. Hence, the extensive results have proved it has mitigated computational and communication burden. Elmisery et al. [30] have developed new IoMT devices with respect to fog nodes. The prime aspect of this model was to manage the privacy and confidentiality of patient's data. With an integration of such models, the proposed scheme was measured, and its outstanding results have proved that the efficient performance.

1.2. Chronological Review

Figure 1 depicts the chronological analysis of existing secure and privacy of data using various methodologies. Here, it takes the recently implemented papers for obtaining the features and challenges of security in IoMT applications. Thus, 10%, 20%, 30% and 40% of literature works considered for the year 2018, 2019, 2020 and 2021, respectively.

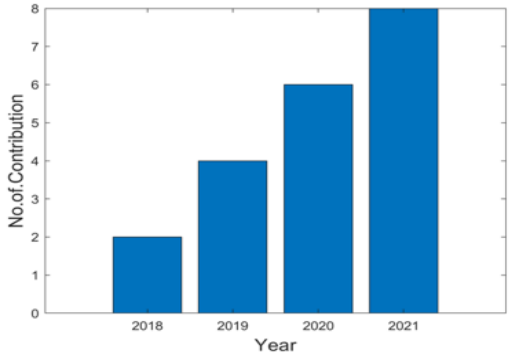

Figure 1. Chronological review on the traditional models of secure and privacy of data in IoMT

2. Introduction to Medical Devices in IoT with Algorithms for Security and Privacy of Data along with Performance Measures

2.1. Introduction to Medical Devices in IoT

IoMT is comprised with medical smart devices, which is all connected to other over the Internet. The prime objective of IoMT application is to handle the medical information. Hence, the Figure 2 represents the general diagram IoT devices along with servers, medical devices and IoT devices.

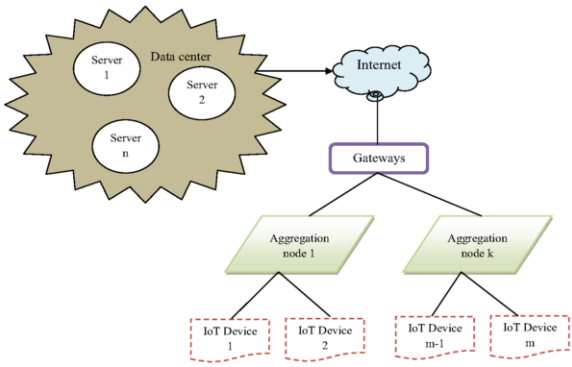

Figure 2. General diagram of IoT network with medical devices

The IoMT communication is another factor to deliberate the data transmission in four ways such as "Body Area Networks, Home Area Networks, Neighbourhood Area

Networks, and Wide Area Networks". Recently, the body area network has become the emerging way of communication with IoMT devices. Some health records of individuals are gathered through the wearable body sensors, which is then transmitted via Internet and presented in the IoMT application. The diagrammatic illustration of body area network is depicted in Figure 3.

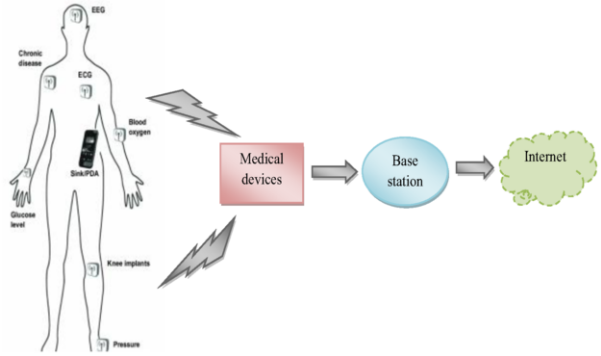

Figure 3. Diagrammatic representation of body area network with IoMT Devices

2.2. Algorithmic Categorization on Security and Privacy of Data

This section elucidates the algorithmic categorization for data security and privacy over IoMT platform. Various standard approaches have been utilized to increase the system efficiency. It is mainly focuses on the methodologies of authentication process, encryption and decryption algorithm, and blockchain based techniques. Thus, the Fig. 4 shows the algorithm categorization for privacy preserving the data in IoMT sector.

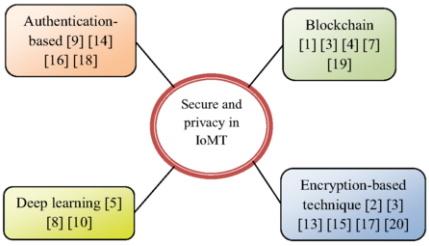

Figure 4. Secure and privacy preserving algorithm for IoMT data

2.3. Performance Measure

In order to validate the efficacy of the model, diverse number of performance measures is taken. Here, the validation ensures the efficiency and robustness of the system and reduces also the overhead complexity in terms of computation, storage and communication. Table 1 illustrates the performance measure that is used for analyzing the various techniques.

Table 1. Diverse performance Metrics taken for validating the security and privacy of data in IoMT applications

Article	Communication overhead	Computation overhead	Storage cost or overhead	Response time	Accuracy	PSNR	Throughput	Miscellaneous measures
[1]	-	-	-	-	-	-	-	Scalability, security, privacy, storage size, execution time
[2]	-	-	-	-	-	✓	-	SSIM, RMSE, MSE and time complexity
[3]	-	-	-	-	-	-	-	Power consumption, transaction speed, scalability
[4]	-	-	-	✓	✓	-	-	Latency ratio, precision, trust
[5]	✓	✓	-	-	-	-	-	-
[6]	✓	✓	-	-	-	-	✓	Delay, packet delivery rate
[7]	-	-	✓	✓	-	-	-	-
[8]	-	-	-	-	-	-	-	ROC curve
[9]	✓	✓	✓	-	-	-	-	-
[10]	-	-	-	-	-	✓	-	Entropy, SSIM
[11]	-	-	-	-	✓	-	-	Running time
[12]	-	-	-	-	-	-	✓	Packet loss ratio, energy consumption, delay, link breaches
[13]	✓	✓	-	-	-	-	-	Running time
[14]	-	-	-	-	✓	-	-	Precision and recall
[15]	-	-	-	-	-	-	-	Authentication and key agreement security
[16]	✓	✓	-	-	-	-	-	-
[17]	-	-	-	-	-	-	-	-
[18]	-	-	-	-	-	-	-	Energy security level
[19]	✓	✓	-	-	-	-	-	-
[20]	-	-	-	-	✓	-	-	Running time, key generation

3. Features, Research Gaps and Future Challenges for Security and Privacy of Data for IoMT Devices

3.1. Features and Challenges on Existing Works

Table 2 elaborates the advantages and disadvantages related to existing works of secure and privacy of data in IoMT applications. Over the past few years, different expertise deploys distinct approaches to analyze the security performance.

3.2. Challenges and Further Research

This section explains the challenges related for security and privacy of data from IoMT. Over IoMT applications, some challenges are prominently visible that degrade the performance, efficiency and robustness. The prime challenging issue [31] is lack of

standardization for medical devices. Some of the most constraint factors that degrade the efficacy of the systems are scalability, reliability, insecurity, data integrity, consistency and efficiency. The challenges are listed as below while deploying the IoMT devices.

- ***Revealing the patient information:*** The reputation of healthcare institutions and the well-being of their patients are both severely compromised.
- ***Data insecurity:*** Due to the fact that these tools are being used in a diverse set of locations, including in hospitals, care homes, and remote care and the poor competence of patients in regards to security, there is a great chance that in home care and remote care, the patient's data would be targeted by hackers. In similar way, the patient's health data can be easily leaked [32] from the hospital from the insiders too. Thus, the challenge is to develop the efficient authentication and authorization mechanism in future perspective.

Table 2. Merits and demerits noted from literature works on security and privacy of data in IoMT devices

Author Name	Algorithm	Merits	Demerits
Kumar and Tripathi [12]	Consortium blockchain	• It enhances the decentralization of the system. It improves the scalability measure to preserve the data.	• Being usage of distributed cluster, it limits with computation time complexity.
Ogundokun *et al.* [13]	Cryptography and steganography	• It becomes feasible as it improves the robustness of the system. It reduces the time complexity	• It does not support the data related to audio or video formats. It suggests using learning approach for further improvement.
Mohan et al. [11]	ECC and blockchain	• It increases the scalability and mitigates the power consumption.	• Software application is not supported for this model.
Abbas et al. [14]	Blockchain	• It attains the impressive results regarding distinct measures.	• It may fails with structural and computation issues.
Wang et al. [15]	SVM	• It enhances the system efficiency by achieving less cost effective	• It is not applicable for real-world applications.
Sun et al. [16]	Routing	• It reduces the computational overhead for both encrypting and decryption the information	• It is suggested to include advanced techniques to achieve higher results.
Egala et al. [17]	Blockchain	• It exploits the low latency value	• It does not consider some QoS constraints for performance improvement
Aslam et al. [18]	KNN	• It improves the predictive results.	• The usage of ANFIS tends occurring the structural complexity.

- ***Data flaws:*** By having enormous number of medical data, data handling becomes another challenging factor as it has the chances to misplace the data to

another patient [33]. Hence in the future, it is motivated to develop computer-aided and security-based IoMT device AI models to handle the data efficiently.

- ***Accuracy and privacy:*** Over the IoMT environment, medical data can be accessed by various malicious actors as it presents huge security concerns regarding confidentiality, integrity, and accuracy. Due to attack intrusion [34], the medical data may get lost or altered. Therefore, a well-developed method, such as an intrusion detection system, must be implemented to maintain the accuracy and privacy of data.

The protection of the patients' confidentiality and safety is the primary emphasis of IoMT's contributions to healthcare system. Security measures, such as authentication and authorization schemes, are essential to prevent unauthorized access to confidential healthcare information. That's why it's crucial to find a cutting-edge approach that can ensure data is secure during its entire journey. Review findings show that many documented techniques exist to secure IoMT devices. However, traditional cryptography and machine learning based security techniques cannot be implemented on these smart devices because of a number of limitations, including power, size, implantability, and wearability. Therefore, an effective new solution is needed that can fulfil all the security requirements and extend throughout the medical space to assure the security, privacy, and trust of these smart devices. The examination of the surveyed data also shows that the ECC algorithm, lightweight authentication, and the blockchain technique provide the highest levels of security. Therefore, future studies should concentrate on creating effective lightweight cryptography, intrusion detection systems to protect and safeguard data from IoMT devices, making it possible to construct power-efficient and sustainable IoMT devices.

4. Conclusion

This survey has illustrated the different methodologies used for security and privacy of data of IoMT devices. The basic introduction along with contribution has given, which was followed by providing the literature works. The chronological analysis was done by the recent deployed works related for the security and privacy of IoMT data. Consequently, the survey work has been analyzed with diverse performance metrics, algorithm implementation, merits and demerits. Finally, the insights of survey have rendered the challenging concerns that lead to future development.

5. Acknowledgement

This work has been carried out in the context of the research project Digi Remote, funded by the Research Council of Norway in the IKTPLUSS program, grant number 310137.

References

[1] Yu S, Park K. SALS-TMIS: Secure, Anonymous, and Lightweight Privacy-Preserving Scheme for IoMT-Enabled TMIS Environments. IEEE Access, 2022; 10: 60534-60549.

[2] Al-Otaibi YD. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. Computers and Electrical Engineering, Jul 2022; 101(C). https://doi.org/10.1016/j.compeleceng.2022.108129.

[3] Changa J, Ren Q, Ji Y, Xu M, Xue R. Secure medical data management with privacy-preservation and authentication properties in smart healthcare system. Computer Networks, 20 July 2022; 212: 109013.

[4] Wu G, Wang S, Ning Z, Li records J. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. IEEE Internet of Things Journal, 1 June 2022; 9(11): 8091-8104.

[5] Othman SB, Almalki FA, Chakraborty C, Sakli H. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. Computers & Electrical Engineering, April 2022; 101(2). DOI: 10.1016/j.compeleceng.2022.108025.

[6] Mangla C, Rani S, Herencsar N. An energy-efficient and secure framework for IoMT: An application of smart cities. Sustainable Energy Technologies and Assessments. 2022; 53.

[7] Kaur M, Singh D, Kumar V, Gupta BB, El-Latif AAA. Secure and Energy Efficient-Based E-Health Care Framework for Green Internet of Things. IEEE Transactions on Green Communications and Networking, September 2021; 5(3): 1223 - 1231. DOI: 10.1109/TGCN.2021.3081616

[8] Rahman MS, Alabdulatif A, Khalil I. Privacy Aware Internet of Medical Things Data Certification Framework on Healthcare Blockchain of 5G Edge. Computer Communications, 2022; 192: 373-381.

[9] Rasool RU, Ahmad HF, Rafique W, Qayyum A, Qadir J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. Journal of Network and Computer Applications January 2022; 201(1):103332. DOI: 10.1016/j.jnca.2022.103332.

[10] Kumar V, Mahmoud MS, Alkhayyat A, Ahmad JSM, Kumari A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. J Supercomput. 2022;78(14):16167-16196. doi: 10.1007/s11227-022-04513-4. Epub 2022 May 2.

[11] Mohan D, Alwin L, Neeraja P, Lawrence KD, Pathari V. A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. J Reliable Intell Environ (2021). https://doi.org/10.1007/s40860-021-00153-2

[12] Kumar R, Tripathi R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. The Journal of Supercomputing, 2021; 77: 7916-7955,.

[13] Ogundokun RO, Awotunde JB, Adeniyi EA, Ayo FE. Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia Tools and Applications, 2021; 80: 31705–31727.

[14] Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Pers Ubiquit Comput (2021). https://doi.org/10.1007/s00779-021-01583-8.

[15] Wang J, Wu L, Wang H, Choo K-KR, He D. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. IEEE Internet of Things Journal, 2021 Jan.1; 8(1): 458-473, 1.

[16] Sun J, Khan F, Li J, Alshehri MD, Alturki R, Wedyan M. Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things. IEEE Internet of Things Journal, 2021 Nov.1; 8(21): 15663-15671, 1.

[17] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. IEEE Internet of Things Journal, 2021, 15 July15; 8(14): 11717-11731.

[18] Aslam B, Javed AR, Chakraborty C, Nebhen J, Raqib S, Rizwan M. Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. Pers Ubiquitous Comput. 2021 Jul 22;1-17. doi: 10.1007/s00779-021-01596-3.

[19] Li J, Su Z, Guo D, Choo K-KR, Ji Y. PSL-MAAKA: Provably Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. IEEE Internet of Things Journal, 2021 Sept.1; 8(17): 13183-13195.

[20] Ding Y, et al. DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. IEEE Internet of Things Journal, 2021 Feb.1; 8(3): 1504-1518.

[21] Guan Z, Lv Z, Du X, Wu L, Guizani M. Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach. Future Generation Computer Systems, 2019; 98: 60-68.

[22] Saba T, Haseeb K, Ahmed I. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. J Infect Public Health. 2020 Oct;13(10):1567-1575. doi: 10.1016/j.jiph.2020.06.027. Epub 2020 Jul 15.

[23] Sowjanya K, Dasgupta M, Ray S. Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things. Journal of Information Security and Applications May 2021;58(4):102761. doi: 10.1016/j.jisa.2021.102761.
[24] Alsubaei F, Abuhussein A, Shandilya V, Shiva S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. December 2019; 8: 100123.
[25] Chen F, Luo Y, Zhang J, Zhu J, Zhang Z, Zhao C, Wang T. An infrastructure framework for privacy protection of community medical internet of things. World Wide Web, 2018; 21: 33-57.
[26] Aghili SF, Mala H, Shojafar M, Peris-Lopez P. LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT. Future Generation Computer Systems, 2019; 98: 410-424.
[27] Yi H, Nie Z. On the security of MQ cryptographic systems for constructing secure Internet of medical things. Personal and Ubiquitous Computing, 2018; 22: 1075-1081.
[28] Rani SS, Alzubi JA, Lakshmanaprabu SK, Gupta D, Manikandan R. Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. Multimedia Tools and Applications, 2020; 79: 35405-35424.
[29] Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJPC, Park Y. BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access, 2020; 8: 95956-95977.
[30] Elmisery AM, Rho S, Aborizka M. A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. Cluster Computing, 2019; 22: 1611-1638.
[31] Nandy S, Adhikari M, Khan MA, Menon VG, Verma S. An Intrusion Detection Mechanism for Secured IoMT Framework Based on Swarm-Neural Network. IEEE Journal of Biomedical and Health Informatics, May 2022; 26(5): 1969-1976.
[32] Guo R, Yang G, Shi H, Zhang Y, Zheng D. O3-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System. IEEE Internet of Things Journal, June 2021; 8(11): 8949-8963.
[33] Alqaralleh BAY, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Pers Ubiquit Comput, Feb 2021. https://doi.org/10.1007/s00779-021-01543-2
[34] Wang Y, Zhang A, Zhang P, Qu Y, Yu S. Security-Aware and Privacy-Preserving Personal Health Record Sharing Using Consortium Blockchain. IEEE Internet of Things Journal, July 2022; 9(14): 12014-12028.