Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends

Thavavel Vaiyapuri[1], Adel Binbusayyis[2*], Vijayakumar Varadarajan[3]

College of Computer Engineering and Science[1,2],
Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
Centro de Tecnologia,Federal University of Piauí, Brazil[3].

***Abstract*—In the past decades, healthcare has witnessed a swift transformation from traditional specialist/hospital centric approach to a patient-centric approach especially in the smart healthcare system (SHS). This rapid transformation is fueled on account of the advancements in numerous technologies. Amongst these technologies, the Internet of medicals things (IoMT) play an imperative function in the development of SHS with regard to productivity of electronic devices in addition to reliability, accuracy. Recently, several researchers have shown interest to leverage the benefits of IoMT for the development of SHS by interconnecting with the existing healthcare services and available medical resources. Though the integration of IoMT within medical resources enable to revolutionize the patient healthcare service from reactive to proactive care system, the security of IoMT is still in its infancy. As IoMT are mainly employed to capture extremely sensitive individual health data, the security and privacy of IoMT is of paramount importance and very crucial in safeguarding the patient life which could otherwise adversely affect the patient health state and in worse case may also lead to loss of life. Motivated by this crucial requirement, several researchers in tandem to the advancement in IoMT technologies have continuously made noteworthy progress to tackle the security and privacy issues in IoMT. Yet, many possible potential directions exist for future investigation. This necessitates for a complete overview of existing security and privacy solutions in the field of IoMT. Therefore, this paper aims to canvass the literature on the most promising state-of-the-art solutions for securing IoMT in SHS especially in the light of security, privacy protection, authentication and authorization and the use of blockchain for secure data sharing. Finally, highlights the review outcome briefing not only the benefits and limitation of existing security and privacy solutions but also summarizing the opportunities and possible potential future directions that can drive the researchers of next decade to improve and shape their research committed on safe integration IoMT in SHS.**

Keywords*—Smart healthcare system; internet of medical things; authentication and authorization; security and privacy; blockchain; intrusion detection system

I. Introduction

In recent years, SHS have greatly increased the economy and is considered as essential component of economy. The IoMT performs a crucial role towards the development of SHS by enabling to develop wide range of applications, say telemedicine, smart medication, onsite and remote monitoring of medical resources. patients treatment compliance and behavioral change. The medical devices which are equipped with sensors and interconnected in the healthcare sector are named as IoMT [1]. The workload in hospitals could be decreased by restricting unnecessary hospital visits with the use of IoMT. Also, it provides a safe data transmission environment for interchanging sensitive medical data amongst diverse medical sectors. IoMT's applications have made lives appropriate. The concern of IoMT security, privacy and trust occurs rapidly. security, privacy and trust have recently received more attention among researcher community [2].

In data security, the storage and transmission of the data is secured and safeguarded to ensure the integrity, validity and importantly authenticity of the data. Further, it assures that the data can be viewed and modified only by the authorized users. Privacy-preserving (PP) is another key objective to be considered while designing an SHS. It mainly account for severity and sensitivity of shared data when it is transmitted over an open and insecure channel. PP involves content and contextual requirements. The patient information is protected against any data leakage by content privacy but achieving patient privacy is a challenge because an attacker can recognize patient health state based on the attended doctor's identity. Also, it is crucial to ensure contextual privacy. Contextual privacy involves of protecting the communication's context. In IoMT enabled SHS, various symmetric and asymmetric encryption method are used to achieve privacy [3].

Recently, it is reported in literature that it is not an optimal solution to apply complex machines learning (ML) algorithms on resource-constrained devices such as IoMT [1]. Yet, it can be resolved by deploying simple PP methods on IoMT devices and utilizing the benefits of cloud for complex ML algorithms [4], [5]. Many works are reported in literature based on cloud related securing solutions for IoMT in SHS. This paper aims to introduce the IoMT enabled SHS architecture, summaries various security, privacy and trust mechanisms published in recent years for IoMT enabled SHS. Finally, it concludes presenting few recommendations for future research directions.

II. Review on Security Mechanism for IoMT Enabled SHS

Security of IoMT in SHS plays a significant role when compared to typical IoT-based infrastructures. Recently, extensive research had been done for securing IoMT enabled smart

TABLE I. COMPARISON OF RECENT PROMISING SECURITY MECHANISMS FOR IOMT ENABLED SHS

Security Focus	Authors	Strengths	Weakness
Secure data transmission	Mahender et al [6]	1) Any information concerning the identity and the patient's medical data was not revealed by the system. 2) The system achieved a better security level. 3) To save data transmission, the system was utilized.	It caused some major issues like large computation and also storage costs.
	Elhoseny et al. [7]	The system demonstrated its potential in effectively hiding the sensitive patient data confidentially to a transmitted cover image with higher undetectability and capacity but with minimum degradation in the acquired stego-image.	The system had provided satisfactory results, although, it demonstrate to work effectively.
Secure authentication	Rakesh et al. [8]	The hash variable value did not rely upon the hash functions for improving network security. The latency or delay of the system was not affected by the deviation in hashing.	A safe effective communication was not given by the system.
	Xu Cheng et al. [9]	The system built on community medical IoT system ensured the nodes' legality and communication security.	The system had a high computational expense and less security.
Confidentiality	Xuran Li et al. [10]	1) It protected the patient's confidential medical data amassed by means of medical sensors. 2) The eavesdropping risk was drastically reduced by the system.	It might cause partial perfect secrecy.
Access Control	Xunbao Wang et al. [11]	The system could be protected effectively during access process and transmission without loss in performance.	The manifold identities of the medical staff were not considered by the system.
privacy-preserving	Jing Wang et al. [12]	The system ensures data privacy during model training and also guarantees the security of the trained model.	The ML models are not supported by the system.

healthcare. This section summaries some state-of-the-art works as follows:

Faisal Alsubaei et al. [13] proposed a framework for security assessment of web-based IoMT. The framework recommends security features for IoMT employing ontological scenario-based approach. Also, it is employed to assess the protection and impediment of IoMT approaches. The proposed framework has demonstrated its potential in adapting (1) emerging new technologies and stakeholders; (2) compliance with standards; and (3) granularity. In general, system administrators are responsible for formulating security-related decisions. But the proposed framework opens avenues for all stakeholders in SHS to gain experience in cutting edge technologies related to the field of IoMT security. The system proved its efficacy with evaluation results in terms of all assessment attributes. But the employed assessment attributes were not easy to interpret by novice users like medical staff, patients who lack security and technical knowledge.

Muhammad Asif et al. [14] proposed a technique to ensure privacy of medical data especially against the threats emerging internally within SHS. The system allows access only for authorized users such as doctors and patients to communicate across the physical boundaries. The system had implemented authorization defining the permissions and roles merely for medical staff. Further, the system enabled to remove any conflicts in access control models. Also, it guarantees to provide secure communication amongst doctors and patients in an efficient way. The system proved to outperform when compared with other related recent access control models in literature. However, the system does not facilitate to perform copy and move operations on directory resource.

Jinquan Zhang et al. [15] examined an encrypted storage model and a secure energy-efficient communication utilizing the benefits of rivests cipher 4 (RC4) for electronic health records (EHR) within IoMT enabled SHS. The system employed MedGreen authentication algorithm based on bilinear pair and elliptic curve for establishing secure communication. Also, the system utilized MedSecrecy algorithm that leverages Huffman compression ad RC4 for efficient data storage. The developed algorithm demonstrated to maintain the effectiveness of RC4 encryption and reduce the length of ciphertext data. Also it improved confidentiality, security and randomness. The simulation and analysis results proved that the system was energy-saving, secure and very effective for EHR. But, the system was not suitable to obtain more possible user information. In addition, Table I summarizes the state-of-the art works related to securing IoMT devices and applications in SHS.

III. Review on Lightweight Security Approaches for IoMT

Norah Alassaf et al. [16] proposed a lightweight cryptographic technique for IoMT enabled SHS applications. The contribution investigated the characteristics of SIMON cipher and employed it for IoMT enabled SHS applications for attaining performance as of a practical perspective. The system recommended to add an enhancement via original SIMON cryptography's implementation to diminish the computational complexity incurred owing to encryption. Also it enabled to preserve the practical balance between performance and security. However, the system did not give good results.

Zisang Xu et al. [17] introduced a key agreement and lightweight mutual authentication approach for IoMT. The system without employing symmetric encryption guaranteed to provide forward secrecy. The authors have utilized ProVerif software which is an automatic security verification tool to verify the system's security. The theoretical examination and experiential outcomes signified that the system drastically reduced the computational cost in comparison to the methods based on asymmetric encryption. Also, the system displayed lesser security risk compared to other lightweight approaches. Nonetheless, the system did not present the encryption and decryption time precisely.

Jianfei Sun et al. [18] proffered a lightweight fine-grained access control method to preserve the data privacy in IoMT enabled SHS. For the successful transformation of access policy and user attributes to the corresponding shorter length vectors, the system employed the optimized vector transformation process, whilst the other processes delivered longer and redundant vectors. This system was very significant in reducing the cost overhead incurred during decryption, key generation and encryption phases. Later, the system employed CP-ABE to gain the benefits of fine-grained access control and lightweight policy hiding to support SHS and handle the offline/online transformation process. Nonetheless, the system did not support traceability and attribute revocation.

Xiuqing Lu and Xiangguo Cheng [19] launched a lightweight data sharing approach with an aim to secure IoMT devices. First, the system ensured to provide authorized access and privacy over the shared data. Second, the system employed effective integrity verification when the user attempts to download the shared data. Doing so, the system enables to avoid false computational outcome or query. At last, the approach achieves lightweight in accomplishing the patients' and users' operation. The security analysis results confirmed that the system can enable to share data securely and effectively in IoMT enabled SHS as well its efficient in terms of computational cost. The system was not flexible towards possible attacks like tag forgery, reader impersonation and message eavesdropping.

Mahdi Fotouhi et al. [20] presented a lightweight 2-factor authentication approach to secure IoMT. The system was secured against different attacks. Furthermore, the system executes the formal and informal security evaluation. The system's security verification had been authenticated via the ProVerif. Moreover, the system had been simulated via the OPNET network simulator and compared with various other methods with regard to performance and security needs. The simulation comparisons and outcomes determined that the system had been appropriate and supported with added security attributes when compared to the relevant approaches. However, the system couldn't exhibit the precise security level.

Ran Ding et al. [21] introduced a lightweight PP identity-based authentication system for IoMT. The system performed data authenticators computation, data integrity verification on edge server. Also, edge server was used to system's computation overload and manage the third-party verification. The system achieved data privacy by enabling the patient to encrypt and transmit healthcare data to edge server. Also, the system uses cloud server to enhance the availability of the patient's data. At last, the performance and security evaluation are conducted to show the system potential. However, the system encompassed a storage overhead issue.

IV. Review on Blockchain Approaches for Security IoMT

Seyed Morteza et al. [22] presented an effective and secure method called "MedSBA" for storing medical data in SHS. The method is based on blockchain technology to ensure user privacy. Also, the system attempts to achieve fine-grained access control over patient data employing attribute based encryption (ABE) in compliance to the general data protections regulation. The system employed private blockchain to revoke the instant access which is very challenging in ABE. The security is proven via the formal design, whilst, the system's functionality had been proven using BAN logic. The efficiency of the system with regard to computational complexity and storage is demonstrated by simulating MedSBA's using OPNET software. Nonetheless, the system did not support the exchange of cryptocurrency between the data consumer organizations and the individuals for data sharing.

Ashutosh Sharma et al. [23] proffered a blockchain approach integrating the benefits of smart contracts for IoMT. The system examined the dimensions which the smart contract and decentralization could provide in IoMT. The IoMT devices are deployed in appropriate place to capture the data concerning the application needs. Also, these IoMT devices are pre-programmed to process and transmit the captured data. The efficiency of the system is demonstrated in comparison to other related techniques in terms of performance parameters such as average latency, average energy efficiency and average packet delivery ratio. However, the system encompassed less service quality; it did not function efficiently.

Neha Garg et al.[24] launched an authentication key agreements scheme based on blockchain for IoMT environment, termed as BAKMP-IoMT. It offered secured key management among the cloud servers, personal servers and the implantable medical gadgets. Further, the system provides secure access to sensitive healthcare data and ensures that it is accessed only by authorized users. This achieved by storing all the sensitive healthcare data into blockchain which is stored in cloud. Comprehensive formal security analysis has been conducted utilizing the extensively acknowledged automated tool, AVISPA to show the potential of the system against various types of possible attack. The comparative analysis results indicated the efficacy of the proposed method, BAKMP-IoMT over other existing approaches in terms of security requirements, communication and computation costs.

Jie Xu et al. [25] presented a PP scheme based on blockchain for large scale health data. The scheme encrypts the health data utilizing fine-grained access control. In specific, the user transaction are utilized for key management that can allow the users to add or revoke authorized doctors. Moreover, it avoid medical disputes as doctor diagnosis and IoT data cannot be tampered or deleted once stored to blockchain. Experiential and security evaluation outcomes confirmed that the system can well be applicable for SHS. However, the insider attacks are overlooked by the system.

V. Review on Authentication and Authorization Techniques for IoMT

Venkata P. Yanambaka et al. [26] suggested a lightweight and robust authentication based on physical unclonable function (PUF) for IoMT. This scheme does not stores any IoMT device related data on server memory. The system validation is performed utilizing a hybridized oscillator arbiter PUF. The amount of keys utilized for authentication was approximately 240 based on the PUF used during system validation. The authentication scheme being lightweight can be utilized in several designs for supporting the design's scalability and increasing its robustness. However, the system failed to ensure that the messages from server could be authenticated by the client.

Xu Cheng et al. [9] studied a secure identity authentication for community medical IoT. Here, the authors have utilized node security for system initialization. Next, the identity authentication was developed utilizing the benefits of mechanisms such as signature, session key symmetric encryption, elliptic curve encryption algorithm, secure two-way method. An effective community medical IoT node and an update mechanism that are secure and reliable to update the session and authentication keys is investigated. On the community medical IoT, the nodes' legality, along with the communication security had been ensured by these measures. The scheme was further appropriated for the community medical IoT's scene via the analysis, along with the analogy of experiential performance. However, the system had high computational costs and more power consumption.

Deebak et al. [27] suggested a mutual authentication scheme to secure SHS which centered on the IoMT. The system leveraged cloud to support emergency treatment for patients over internet communication from medical experts. The system ensured to secure the sensitive medical records and also maintained the patient anonymity. Further, it delivered an authentic signature for executing the secured transmission between the communication nodes. But, the system did not ensure to validate the access for services with regard to unforgability, undeniability and verifiability. Also, the system was insecure against confidentiality, forgery of health-report, non-repudiation and patient anonymity.

In [28], Sanaz Rahimi Moosavi et al. recommended a secure and effective architecture based on smart gateways for authentication and authorization architecture in IoMT-enabled SHS. Here, the smart gateways deployed in each healthcare sensors performed authentication and authorization and reduced the sensor overload while maintaining the all security requirements. Notably, the system relied on DTLS handshake protocol which is regarded as key solution for IoT security. The analysis results confirmed that the proposed architecture rendered better security compared to centralized delegation architecture. However, for the possible attacks, the system was not resilient.

Lone et al. [29] introduced a secure communication for medical applications utilizing ABE for authentication in Het-Net. Here, health related data are secured utilizing ABE. This has not only helped to reduce the communication overhead but also has secures health data from intruders [30]. The entire security technique is implemented using high-level protocol specification language (HLPSL). The system codes are validated using automated tool, AVISPA. However, system provided less security and failed to work effectively.

Muhammad Tahir et al. [31] examined a framework for authentication and authorization mechanism which is lightweight to support blockchain-enabled IoT networks existing in health-informatics. Random numbers are utilized in the authentication process that was linked by conditional joint probability. This enabled the system to establish secure connection for the data acquisition amongst IoT devices. The authors utilized automated tools and simulator such as AVISPA and Cooja for system validation and evaluation, respectively. The system had provided strong mutual authenticity along with improved access control. It also decreases both the communication along with computational overhead cost when weighted against others as shown by the experiential outcomes. However, the system provided less efficient.

Yang Xin et al. [32] suggested a multimodal biometric identification scheme in the IoMT. An effective matching algorithm utilized by the system was based on secondary computation of the Fishers vector (FV). Further, the system utilized three different biometric techniques like finger vein, fingerprint and face. These techniques are fused at feature level. Also, the system employed fake feature in the process of feature fusion which arises most frequently in practical scene. For decrementing the cause of the system's accuracy rate, and for increasing its robustness, the fake picture was removed. The designed framework had achieved an improved recognition rate as showcased by the experiential outcomes. It offered higher security whist analogized with unimodal biometric system that are extremely significant for an IoMT platform. But, the system had provided low accuracy values.

VI. Review on Privacy Preserving Approaches for IoMT

Maria et al. [33] proffered a PP approach for IoMT based on elliptic curve digital signature. By edge computing servers, privacy preservation in data transmitted as of IoMT to the cloud is done by this system. Especially, the captured health data was concealed from edge device and the identity of IoMT devices, namely, wearable or smart devices remained anonymous to cloud. As this solution is based on elliptic curves cryptography approach, its implementation on IoMT devices was feasible and affordable. Nevertheless, the computation and communication cost of the system found to be high.

Dong Zheng et al. [34] recommended an effective PP scheme for sharing medical data in IoT environment. The system supported data sharing leveraging the benefits of ABE. Further, the system utilized the attribute bloom filter removing the attribute matching function to maintain the confidentiality of attributes involved in the access control policy definition. The system utilized offline or online encryption technology in the phase of encryption to enhance the encryption's efficacy. A huge quantity of work ought to be done at the encryption stage before knowing the message. The cipher text could be produced quickly when the message was known. The analysis results demonstrated the potential of the scheme for sharing data in IoT environment. However, the scheme failed to verify and validate the cipher text that was stored over cloud.

Deebak et al. [35] proposed a PP protocol for securing SHS where attacker cannot imitate legal user to gain illegal access to the handheld smart card. The authors have used random-oracle model to perform formal and resource analysis to demonstrate the effectiveness of system security. Moreover, they have built a IoMT enabled SHS with top security feature which was revealed by its performance analysis. For analyzing, the network parameters based on the NS3 simulator, the experimentation analysis was executed. Regarding the throughput rates, packet delivery ratio, routing overhead along with end-to-end delay for the system, the collected results had shown superiority when analogized to other prevailing protocols.

Raylin Tso et al. [36] proffered a PP scheme for data communication through protected multi-party calculation in the HC cloud that are equipped with sensors. The system was based on the FairplayMP framework that enabled programmers to execute such protocols who were not specialist secure computation theory. Additionally, it was appropriate for distributed environments and it supported any numeral of participants. For example, to communicate with n-disparate data servers, each sensor node requires one single secret key to be stored in advance. But, the system was stored with three secret keys in advance in each sensor to communicate with three data servers despite the system offers low-level security.

S. Sheeba Rani et al. [37] presented an optimum users-based secure transmission of data within IoMT. The system employed Chinese Remainders Theorem to produce the cipher text copy according to the chosen number of users. Further the system utilized metaheuristic algorithm to choose the user in IoMT. Through simulation, the secure data performance was proved in terms of computation time, the energy price, etc., The outcomes confirmed that secure data could be effective whilst applied for ensuring security chances in IoT-based SHS but, low security was offered.

Alia Alabdulkarim et al.[38] put forward a privacy preserving single decision tree techniques aimed at clinical decisions-support systems to diagnosis the symptoms without disclosing the patients' data to disparate network attacks on IoT devices. For protecting users' data, homomorphic encryption cipher was utilized. Moreover, for avoiding one party as of decrypting the data of other parties, nonces were utilized as they would utilize the identical key pair. In addition, the system performed better than the Naïve Bayes algorithm by 46.46% which was revealed by the simulation outcomes. Additionally, for showing that it satisfies the attribute value's frequency, hospitals' dataset's privacy requirements, and effectively diagnoses the symptoms, the system was evaluated. However low-security services were possessed by the system.

Rihab Boussada et al. [39] examined a privacy preserving aware data transmission fort IoMT enabled SHS. User pseudonyms as public keys were defined by lightweight Identity-based encryption which was constructed on the elliptic curves discrete logarithm (ECDL) method. The contextual along with content privacy necessities are satisfied by the system. Regarding smart things limited resource nature, it was based on an identity-centered encryption scheme and specific communication scenario. A wide security examination was offered for validating the system and the performance analysis demonstrates its efficacy. However, for the e-HC emergency, the system was inappropriate.

Solihah Gull et al. [40] recommended a reversible data hiding approach based on dual image with large capacity for IoMT based networks. Initially, the Huffman encoding scheme was used to preprocess the captured secret data. A codebook of 'd' bits are generated after Huffman encoding to encode indices which are decimal values. For acquiring dual stenos-images, the indices' value are partition into two parts and embedded into two images that are similar to each other. Though very large payload was shown by the scheme, it proved to maintain the perceptual quality at high level. A noteworthy improvement was offered by the system and also computationally effective that made it to be utilized in the network of IoMT. However, for controlling the underflow and overflow issues, there wasn't an effective strategy.

Pei Huang et al. [41] presented a practical technique that could validate patients with the noisy signal of electrocardiogram (ECG) as well as offered disparate private protection concurrently. Regarding the present moving status, the scheme could identify the motions and adapted the algorithm. By offering indistinguishability, The ECG templates' privacy was protected. The system's effectiveness was analyzed and validated over online datasets. For validating the system, pilot analysis on human subjects was conducted. However, for attacking, the system was not flexible.

Zhiwei Wang et al. [42] inspected an effective blind batch encryption scheme based on Computational Diffie-Hellmans assumption, which could be demonstrated as secure. For secure and privacy preserving medical services in SHC, the system utilized protocol. In the frame of six classic attacks, the system analyzed the protocol and executed prototype in the platform of Intel Edison. The experiments revealed that the system was effective for 'cheap' communication protocols along with resource-limited devices. For limited-storage devices, the system might require a heavy cost.

VII. Conclusion

When the networks are employed at large scales, the major concern is security. The major area focused in IoMT enables SHS is the patients' security and privacy. In this direction, authentication and authorization scheme play a very crucial role in ensuring eavesdropping the sensitive healthcare data and are considered as critical security requirements. Thus, there is great need for effective new solution that can render end-to-end data protection. From the review, it can be observed that several schemes are published for securing IoMT devices. Nonetheless, owing to the several constraints such as power, size, implantable and wearable, these smart devices do not have required resources for implementing the existing machine learning based security schemes. Therefore, to ensure the security, privacy and trust of these smart devices, require an efficient new solution that can meet all the security requirement and span across the design space of cyber. Also, the survey analysis reveals that ECC algorithm, lightweight authentication, and blockchain method are offering best security compared to conventional algorithms. Thus, to build power-efficient and sustainable IoMT enabled SHS, the upcoming research must focus on developing effectual lightweight intrusion detection systems to secure and safeguard IoMT enabled SHS.

Acknowledgment

The authors are very grateful to thank their Deanship of Scientific Research at Prince sattam bin abdulaziz university, Saudi Arabia for technical and financial support in publishing this work successfully.

References

[1] K. K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, and C. Thapa, "Towards a security enhanced virtualised network infrastructure for 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] M. Kumar and S. Chand, "A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10650–10659, 2020.

[7] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for iot-based healthcare systems," *Ieee Access*, vol. 6, pp. 20596–20608, 2018.

[8] R. K. Mahendran and P. Velusamy, "A secure fuzzy extractor based biometric key authentication scheme for body sensor network in internet of medical things," *Computer Communications*, vol. 153, pp. 545–552, 2020.

[9] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, H. Sun, and C. Huang, "Secure identity authentication of community medical internet of things," *IEEE Access*, vol. 7, pp. 115966–115977, 2019.

[10] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing internet of medical things with friendly-jamming schemes," *Computer Communications*, 2020.

[11] X. Wang, F. Chen, H. Ye, J. Yang, J. Zhu, Z. Zhang, and Y. Huang, "Data transmission and access protection of community medical internet of things," *Journal of Sensors*, vol. 2017, 2017.

[12] J. Wang, L. Wu, H. Wang, K.-K. R. Choo, and D. He, "An efficient and privacy-preserving outsourced support vector machine training for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 458–473, 2020.

[13] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "Iomt-saf: Internet of medical things security assessment framework," *Internet of Things*, vol. 8, p. 100123, 2019.

[14] M. A. Habib, C. N. Faisal, S. Sarwar, M. A. Latif, F. Aadil, M. Ahmad, R. Ashraf, and M. Maqsood, "Privacy-based medical data protection against internal security threats in heterogeneous internet of medical things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, p. 1550147719875653, 2019.

[15] J. Zhang, H. Liu, and L. Ni, "A secure energy-saving communication and encrypted storage model based on rc4 for ehr," *IEEE Access*, vol. 8, pp. 38995–39012, 2020.

[16] N. Alassaf, A. Gutub, S. A. Parah, and M. Al Ghamdi, "Enhancing speed of simon: a light-weight-cryptographic algorithm for iot applications," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 32633–32657, 2019.

[17] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[18] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, and R. H. Deng, "lightweight and privacy-aware fine-grained access control for iot-oriented smart health," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6566–6575, 2020.

[19] X. Lu and X. Cheng, "A secure and lightweight data sharing scheme for internet of medical things," *IEEE Access*, vol. 8, pp. 5022–5030, 2019.

[20] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot," *Computer Networks*, vol. 177, p. 107333, 2020.

[21] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable iot-based health storage system," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8393–8405, 2019.

[22] S. M. Pournaghi, M. Bayat, and Y. Farjami, "Medsba: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–29, 2020.

[23] A. Sharma, R. Tomar, N. Chilamkurti, B.-G. Kim, *et al.*, "Blockchain based smart contracts for internet of medical things in e-healthcare," *Electronics*, vol. 9, no. 10, p. 1609, 2020.

[24] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[25] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[26] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[27] B. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things," *IEEE Journal on Selected Areas in Communications*, 2020.

[28] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "Sea: a secure and efficient authentication and authorization architecture for iot-based healthcare using smart gateways," *Procedia Computer Science*, vol. 52, pp. 452–459, 2015.

[29] T. A. Lone, A. Rashid, S. Gupta, S. K. Gupta, D. S. Rao, M. Najim, A. Srivastava, A. Kumar, L. S. Umrao, and A. Singhal, "Securing communication by attribute-based authentication in hetnet used for medical applications," *Eurasip Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 1–21, 2020.

[30] T. Vaiyapuri and A. Binbusayyis, "Application of deep autoencoder as an one-class classifier for unsupervised network intrusion detection: a comparative evaluation," *PeerJ Computer Science*, vol. 6, p. e327, 2020.

[31] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, 2020.

[32] Y. Xin, L. Kong, Z. Liu, C. Wang, H. Zhu, M. Gao, C. Zhao, and X. Xu, "Multimodal feature-level fusion for biometrics identification system on iomt platform," *IEEE Access*, vol. 6, pp. 21418–21426, 2018.

[33] M.-D. Cano and A. Cañavate-Sanchez, "Preserving data privacy in the internet of medical things using dual signature ecdsa," *Security and Communication Networks*, vol. 2020, 2020.

[34] D. Zheng, A. Wu, Y. Zhang, and Q. Zhao, "Efficient and privacy-preserving medical data sharing in internet of things with limited computing power," *IEEE Access*, vol. 6, pp. 28019–28027, 2018.

[35] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, pp. 135632–135649, 2019.

[36] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," *Journal of Signal Processing Systems*, vol. 89, no. 1, pp. 51–59, 2017.

[37] S. S. Rani, J. A. Alzubi, S. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmission on the internet of healthcare things (ioht) with lightweight block ciphers," *Multimedia Tools and Applications*, pp. 1–20, 2019.

[38] A. Alabdulkarim, M. Al-Rodhaan, T. Ma, and Y. Tian, "Ppsdt: A novel privacy-preserving single decision tree algorithm for clinical decision-support systems using iot devices," *Sensors*, vol. 19, no. 1, p. 142, 2019.

[39] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "Privacy-preserving aware data transmission for iot-based e-health," *Computer Networks*, vol. 162, p. 106866, 2019.

[40] S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting huffman encoding with dual images for iomt based healthcare," *Computer Communications*, vol. 163, pp. 134–149, 2020.

[41] P. Huang, L. Guo, M. Li, and Y. Fang, "Practical privacy-preserving ecg-based authentication for iot-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9200–9210, 2019.

[42] Z. Wang, "Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9555–9562, 2019.