IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 9, September 2020, ||Series -I|| PP 51-55

A Survey and Analysis of Security Schemes in Internet of Things for Healthcare Applications

Ms.Hemalatha.K[1], Dr.P.Vijayakumar[2]

[1]Assistant Professor ,Department of Computer Science,KG College of Arts and Science,Coimbatore,India
[2]Associate Professor&Head, Department of Computer Applications,Sri JayendraSaraswathyMaha Vidyalaya College of Arts and science.Coimbatore,India

ABSTRACT-Internet-of-Things (IoT) has revolutionised the medical and healthcare sector through efficient healthcare applications and services for remote healthcare interface between the patients and medical experts. Still, the IoT based healthcare services are prone to several limitations because of the openness and pre-determined architecture paving way for security threats and attacks. Many studies have analysed these vulnerabilities and established security schemes for authentication, access control and privacy preservation. This paper has conducted a survey of the recent security schemes developed for the IoT healthcare applications with the goal of understanding the various security mechanisms, their features and also their vulnerabilities. The principle mechanisms of these security schemes have been analysedand their limitations are also highlighted. Finally, some suggestions for formulating the future research directions are also providedbased on the open issues and challenges.

KEYWORDS: Internet of Things, Healthcare, Wireless Body Area Networks, Remote health monitoring, Authentication, Encryption, Privacy preservation.

I. INTRODUCTION

Internet-of-Things (IoT) has accomplishedcomprehensive acceptance in many sectors and is being adopted into all prominent technologies [1]. The ability to connect different smart objects in a network model to ensure data collection and communication has provided significant achievements. The smart sensors and routers have improved the effectiveness and expansion of the wireless sensor networks to multiple application sectors. The contact-less and efficiency of data retrieval systems through these smart devices has enabled the development of various real-time IoT based applications and services that adhere with the daily public activities. The IoT applications are compliant with the principle rules of data processing namely the volume, veracity, velocity and variety of the data. These rules are strictly followed in the design process of IoT. Irrespective strict design rules, the IoT techniques have introduced innovative applications and have been effective in many modern problems. Still the IoT techniques have certain threats such as privacy attacks, service denial attacks and expensive architectures. These threats form the basis for new innovations which would help in tackling the ill-effects of such drawbacks.

The advanced communication paradigms in IoT and the utilization of smart objects are the part of internet in the modern daily life. This high communication and computing improvements have provided the opportunity to design useful applications but has also raised the security concerns. The smart objects are vulnerable to security risks especially the malicious attacks. The two primary security issues are the physical security for these objects, and the data confidentiality and privacy problems in the IoT data collection process. Emergence of these security risks has demanded the application developers to design novel security measures for the novel innovative applications based on IoT. The security mechanisms required must be highly effective than the traditional mechanisms since the traditional mechanisms are supportive for only the general networks and not the smart objects. Hence the security in IoT becomes one of the hot research topics and has been sought greatly for the broad applications of IoT.

II. IOT IN HEALTHCARE SECTOR

With the flourishing IoT, smart healthcare applications are emerging at a greater speed. The last decade has paved the way for developing body area network (both wired and wireless) [2] which have significantly increased the adoption of smart technologies to provide reliable and convenient healthcare to all people including the geographically distant remote patients. With the development of IoT in this decade, the future of medical sector is inching towards a virtual medical environment. IoT technologies provide competent structured approaches for the healthcare field to remodel the traditional treatment process into an internet based IoT application. As healthcare is one the fast growing and vital industry for the mankind, the modern technologies is developed with greater focus on this sector [3]. The wearable sensors and embedded devices are the primary technologies for this vision. These devices aid the remote doctors in gathering the patients' health data namely temperature, blood pressure, heart rate, pulse rate, etc. these collected data are transmitted through the wireless mediums or internet and the doctors diagnose the patient from their location. The medical treatment is provided through telemedicine. This setting has transformed the entire medical sector.

With the improvements and benefits of IoT healthcare systems, they also suffer from serious security issues [4]. The open nature of the Wireless Body Area Networks (WBAN) and IoT networks provide easy access to all the patients and users along with the adversaries. The adversaries who seek to manipulate the medical communication might access the networks and extract the data which may be illegally processed, dropped or corrupted to their advantages. The intrusion detection and prevention systems were used traditionally in all networks but they lack the edge against the adversaries in IoT [5]. Modern studies have great interest in analysing these security loopholes and identifying effective measures to tackle them. To tackle such attackers, the IoT and WBAN networks started employing security schemes, encryption algorithms, authentication protocols; access control mechanisms and privacy preserving approaches with different extend of impact. Many studies have been conducted in recent years to develop efficient security schemes for IoT healthcare applications. This paper aims at summarizing some of the prominent studies that developed such strategies. In this paper, a survey has been conducted on the recent security schemes presented for the healthcare applications. Also, the discussed schemes are analysed for understanding their features and highlighted their merits and demerits.

III. HEALTHCARE SECURITY SCHEMES

Massive benefits of healthcare applications in IoT and WBAN have paved the way for extensive research in the recent years. With the ever-increasing need for secured communication technologies in medical sector, studies have been conducted to fill the loopholes in the current models. Wang and Zhang [6] designed Bilinear pairing based anonymous authentication scheme in which the adversaries are averted without the linking process. Although it has better computation cost, the storage problems are aplenty in this scheme. Yeh[7]developed two authentication schemes with robust crypto-primitives for building confidential communication mechanism for securing the IoT-WBAN healthcare system. The two authentication schemes were based on SHA-3 and Elliptical curve cryptography (ECC) based scalar multiplication operations with crypto-hash modules for solving the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). Although, the security is improved with user-acceptable computation cost, these authentication models have greater impact on increasing the computation time in practical implementations.

Li et al. [8] proposed anonymous mutual authentication and key agreement scheme with the local server/hub node. This scheme reduced the authentication overheads in terms of storage and computation. However, this model has limited privacy preservation of the collected patient data.Elhoseny et al. [9] presented a hybrid optimization based ECC for enhancing the security of medical images in IoT. This hybrid model consists of grasshopper optimization and particle swarm optimization, which is used to select the optimal key in ECC. This model uses less memory and reduces the computation costs. However, this approach has limited performance towards protection against replication attacks.Shakeel et al. [10] proposed a security and privacy-preserving scheme using learning based deep-Q-networks (LDQN) which maintains the privacy in patient data and also reduces the impacts of malware attacks. The computation and time complexity of this model is comparatively reduced by the multi-layer learning of the medical data. The learning of the traffic features increases the attack detection accuracy and minimizes the error rate. Irrespective of these advantages, this model has limitations in handling multiple features of overlapping attack categories.

Kumar et al.[11] proposedanonymous and privacy-preserving biometrics based authentication scheme for gadget-free healthcare systems. This authentication scheme is developed for the future hyper-connected healthcare environments for patients and elderly people. The security, reliability and anonymity of this scheme against various attackswere verified using formal and informal verification techniques with better computation and communication costs. However, in some adverse conditions, this authentication scheme faces stochastic problems due to the gadget free nature.Aghili et al. [12]designed Lightweight authentication, access control and ownership transfer (LACO) scheme using the three-factor authentication and privacy preserving access controls. This model also considers the ownership transfer considerations from the patients to the doctors to avoid the privacy breach. To avoid the vulnerabilities against the denial-of-service attacks, formal security analysis has been conducted. Although, this protocol increases the security and privacy preservation with limited computation cost, this model has limitations on the quality-of-service (QoS) provided to the patients.

Xu et al. [13] introduced aPrivacy-preserving Medical Recommendation (PPMR) scheme using the Modified Paillier cryptosystem and Dirichlet distribution. This scheme preserves the patient data and also provides recommendation based on similarity and doctors' reputation scores. In this process, the PPMR scheme also identifies the malicious user feedbacks to avoid forged reputation scores. The recommendations are secure and accurate but this model has been found to be efficient for larger networks while for smaller networks, the recommendations require more computation time.Huang et al. [14] presented privacy-preserving ECG-based authentication for the healthcare applications. This model increases the reliability of the long-term health monitoring by maintaining sensitivity and accuracy preservation of the ECG signals. This model effectively detects the movements of the patients through Singular Vector Decomposition (SVD) and uses the ECG based authentication to secure the data. It has high efficiency with effective noise tolerance and privacy preservation but this model has been tested only on human generated noise whose density is greatly different from the generated noise.Xu et al. [15] presented lightweight mutual authentication and key agreement scheme for transmission secrecy without asymmetric encryption. This lightweight scheme has high security which prevents the adversary to extract the previous session keys even if the adversary compromises the sensor nodes. This scheme reduces the computation time and communication cost. However, this scheme has higher computation cost due to the impersonation attacks.

Li et al. [16] developed ECC based three-factor user authentication protocol utilizing the fuzzy commitment scheme for processing the biometric data of wireless medical sensor networks (WMSN). This protocol ensures forward secrecy and increases the authentication efficiency. It also enables the balancing the feature of local password verification and mobile attacks using fuzzy verifier and Honey list techniques. It provides higher level of security and reduced computational cost but has limitations in anonymity. Han et al. [17] introduced atrust-based key distribution scheme with self-healing and SVD based authentication. The key management is hierarchical and hence provided deterministic security and access control. The polynomial based self-healing group key distribution method enhances the secrecy. Although this scheme reduces the storage, computation and communication overheads, it has limitations in handling the replication attacks.Deebak et al. [18] developedSecure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) with a defensive strategy of the fuzzy verifier. This scheme provided better resource utilization of storage, computation, and communication. Although the packet delivery ratio is better in this scheme, the congestion is high due to the proportional addition of more sensors.

Wang et al. [19] proposed blind batch encryption scheme based on the computational Diffie-Hellman (CDH) assumption for healthcare privacy preserving and security. This scheme provides high security against most of the attacks and ensures there is no privacy breach. However, the limitation of this scheme is the higher storage cost. Likewise there is vulnerability in this scheme as the adversary may learn the power usage data of the patients.Vijayakumar et al. [20] developed secure anonymous authentication with trusted authority for ensuring location privacy. This authentication model employs the trust model based signature verification. The location of the patients are preserved and exposed only to the authentic doctors through the Chinese Remainder Theorem (CRT). Although the location privacy is enhanced along with better computation cost and time, this scheme provides only public authentication for the patients unlike the batch authentication.Xu et al. [21] proposed a blockchain-based privacy preserving scheme called Healthchain. This scheme decouples the encrypted data and the keys to ensure adaptive key management. It also provides facility to revoke the doctors' connection any time to enhance the privacy. This approach reduces the transaction size, storage cost and computation overheads, but it creates inconsistency in storage capacities.

Khan et al. [22] proposed a secure authentication and encryption framework using Improved ECC. In this work, the ECC is improved by generating an additional secret key for effective encryption. Along with the Improved ECC, the Substitution-Ceaser cipher is used based on the SHA-512 algorithm. This secured framework has provided less computation cost, encryption and decryption times. However, this model has limitations in handling the mobility data of the patients.Yazdinejad et al. [23] developed decentralized authentication scheme using blockchain to reduce the delays in the critical healthcare systems. This approach consumes less computational cost, storage, time overhead and energy and increases the throughput. This approach also does not require re-centralization which significantly reduces the overhead. However, this scheme lacks decisive strategy for acting faster in emergency situations.Sun et al. [24] developed lightweight policy-hiding ciphertext policy attribute based encryption (CP-ABE) scheme for fine-grained access control mechanism. This mechanism includes an optimized vector transformation approach for modelling the access policies and user attribute set. Then the encryption model is developed through the transformation and computation technology. This mechanism provides high privacy preservation and also reduces the computation overhead. But this mechanism does not protect against the replay attacks.Kumar and Gandhi [25] presented enhanced Datagram transport layer security (DTLS) with constrained application protocol (CoAP)-based authentication scheme. This CoAP-DTLS scheme enhanced the security against many attacks especially the denial-of-service attacks. However, this scheme has limitations in handling mobile users.

The literature studies provided the understanding of different security mechanisms in IoT and WBAN based healthcare applications. From the studies, it is inferred that the healthcare security schemes have many difference from the general security schemes and hence the effectiveness of the schemes is very important for emergency situations. It is learnt that the schemes discussed above have provided efficient results but have certain limitations. These limitations form the motivation and research gap for future researches. In future, the security schemes must be developed by considering the prominent limitations identified in this section.

IV. OPEN ISSUES AND POSSIBLE SOLUTIONS

The IoT healthcare security schemes described in the previous section have been capable of delivering promising enhancements to the security models. Still there are some open challenges in those schemes which might haunt the future real-time applications. Analysing the major issues might be significant for the long-term application designing. The prominent schemes discussed were the blind batch encryption scheme [19], secure anonymous authentication with location privacy [20] and Improved ECC based authentication framework [22]. The blind batch encryption scheme has utilized the CDH assumptions for ensuring the privacy and security. This model is effective against most attacks and prevents the intruders from breaching the privacy policies. But this model has high storage cost and vulnerability in power usage data privacy. To tackle such limitations, the authentication scheme must be tweaked such that there will be two layers of user access priority. Only the authentic and administrative users will be assigned high priority and allowed complete access. The other users in the network will be partially allowed to reduce the intrusion by attackers in disguise as normal users. Another possibility is to reduce the hash chain bits adaptively to accommodate the limited storage.

The secure anonymous authentication schemewith location privacy has used a trusted authority signature verification to tackle the intrusion of non-registered users. This model reveals the location only to the authentic users but protects it from other common users. Still this approach cannot provide personalised batch authentication. This might negatively impact the security efficiency and hence require careful analysis. To overcome such limitations, the batch authentication can be provided to all authentic users based on their past history and current priority. Another solution can be to include selective monitoring agents in the data processing modules to ensure that the users are authentic and then allot specialized authentication keys to them. Similar to this scheme, the Improved ECC based scheme has provided benefits of less computation cost, encryption and decryption times and also increased the security of the user data. However, this scheme finds it difficult to handle the users with mobility. Since not all the patients are critical in a network, the patients might move around their locations. The modern IoT devices are equipped with ability to handle minor movements of the patients. But when the patients are on movements with larger motions, the user data might be lost or corrupted due to the noise. In such cases, the data collection paradigm of the application can be improved through the integration of user and device interface layers. The movements of patients are common in those using wearable sensors and this interface model can reduce the fluctuations. Another possibility is combining different authentication schemes into a hybrid model can be helpful in providing powerful authentications even in the presence of mobility issue. Apart from the individual problems, there are some common problems such as reducing the memory, computation and communication costs commonly in all the schemes. It can be achieved through designing adaptable lightweight authentication schemes for the IoT applications.

V. CONCLUSION

This paper has presented a survey and analysis of recent security schemes for the IoT and WBAN healthcare applications. The survey includedsecurity schemes for encryption, authentication, privacy preservation and access control strategy. This survey has provided an overview of the security schemes utilized in those healthcare applications and highlights their advantages and limitations. The analysis of these features helps in understanding the shortcomings in modelling security schemes and focuses on encouraging the readers to develop efficient, secure healthcare applications that overcome these limitations. It is also intended to develop asecurity scheme using advanced authentication and privacy preserving technologies to tackle all major limitations and enhance the overall performance, in future.

REFERENCES

[1]. Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). “Internet of Things (IoT): A vision, architectural elements, and future directions.” Future generation computer systems, 29(7), 1645-1660.

[2]. Khan, J. Y., &Yuce, M. R. (2010). “Wireless body area network (WBAN) for medical applications.” New developments in biomedical engineering, 31, 591-627.

[3]. Dhanvijay, M. M., & Patil, S. C. (2019). “Internet of Things: A survey of enabling technologies in healthcare and its applications.” Computer Networks, 153, 113-131.

[4]. Khan, M. A., & Salah, K. (2018). “IoT security: Review, blockchain solutions, and open challenges.” Future Generation Computer Systems, 82, 395-411.

[5]. Al‐ Turjman, F., &Baali, I. (2019). “Machine learning for wearable IoT‐ based applications: A survey.” Transactions on Emerging Telecommunications Technologies, e3635.

[6]. Wang, C., & Zhang, Y. (2015). “New authentication scheme for wireless body area networks using the bilinear pairing.” Journal of medical systems, 39(11), 136.

[7]. Yeh, K. H. (2016). “A secure IoT-based healthcare system with body sensor networks.” IEEE Access, 4, 10288-10299.

[8]. Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V., & Choo, K. K. R. (2017). “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks.” Computer Networks, 129, 429-443.

[9]. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., &Arunkumar, N. (2018). “Hybrid optimization with cryptography encryption for medical image security in Internet of Things.” Neural computing and applications, 1-15.

[10]. Shakeel, P. M., Baskar, S., Dhulipala, V. S., Mishra, S., & Jaber, M. M. (2018). “Maintaining security and privacy in health care system using learning based deep-Q-networks.” Journal of medical systems, 42(10), 186.

[11]. Kumar, T., Braeken, A., Jurcut, A. D., Liyanage, M., &Ylianttila, M. (2019). “AGE: authentication in gadget-free healthcare environments.” Information Technology and Management, 1-20.

[12]. Aghili, S. F., Mala, H., Shojafar, M., & Peris-Lopez, P. (2019). “LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT.” Future Generation Computer Systems, 96, 410-424.

[13]. Xu, C., Wang, J., Zhu, L., Zhang, C., & Sharif, K. (2019). “PPMR: A Privacy-preserving online Medical service Recommendation scheme in eHealthcare system.” IEEE Internet of Things Journal, 6(3), 5665-5673.

[14]. Huang, P., Guo, L., Li, M., & Fang, Y. (2019). “Practical Privacy-preserving ECG-based Authentication for IoT-based Healthcare.” IEEE Internet of Things Journal, 6(5), 9200-9210.

[15]. Xu, Z., Xu, C., Liang, W., Xu, J., & Chen, H. (2019). “A lightweight mutual authentication and key agreement scheme for medical Internet of Things.” IEEE Access, 7, 53922-53931.

[16]. Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). “A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems.” IEEE Systems Journal, 14(1), 39-50.

[17]. Han, S., Gu, M., Yang, B., Lin, J., Hong, H., & Kong, M. (2019). “A Secure Trust-Based Key Distribution with Self-Healing for Internet of Things.” IEEE Access, 7, 114060-114076.

[18]. Deebak, B. D., Al-Turjman, F., Aloqaily, M., &Alfandi, O. (2019). “An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT.” IEEE Access, 7, 135632-135649.

[19]. Wang, Z. (2019). “Blind Batch Encryption-Based Protocol for Secure and Privacy-Preserving Medical Services in Smart Connected Health.” IEEE Internet of Things Journal, 6(6), 9555-9562.

[20]. Vijayakumar, P., Obaidat, M. S., Azees, M., Islam, S. H., & Kumar, N. (2019). “Efficient and secure anonymous authentication with location privacy for IoT-based WBANs.” IEEE Transactions on Industrial Informatics, 16(4), 2603-2611.

[21]. Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). “Healthchain: A blockchain-based privacy preserving scheme for large-scale health data.” IEEE Internet of Things Journal, 6(5), 8770-8781.

[22]. Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). “A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data.” IEEE Access, 8, 52018-52027.

[23]. Yazdinejad, A., Srivastava, G., Parizi, R. M., Dehghantanha, A., Choo, K. K. R., &Aledhari, M. (2020). “Decentralized Authentication of Distributed Patients in Hospital Networks using Blockchain.” IEEE Journal of Biomedical and Health Informatics.

[24]. Sun, J., Xiong, H., Liu, X., Zhang, Y., Nie, X., & Deng, R. H. (2020). “Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-oriented Smart Health.” IEEE Internet of Things Journal.

[25]. Kumar, P. M., & Gandhi, U. D. (2020). “Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application.” The Journal of Supercomputing, 1-21.

Ms.Hemalatha.K. "A Survey and Analysis of Security Schemes in Internet of Things for Healthcare Applications." *IOSR Journal of Engineering (IOSRJEN)*, 10(9), 2020, pp. 51-55.