STUDY ON AN IOT BASED SECURE HEALTHCARE MONITORING SYSTEM UNING CRYPTOGRAPHY

Mr. Adars U[1]
Research Scholar, Department of ECE, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, TamilNadu & Assistant Professor, Dept. of Computer Science, PMSA PTM Arts & Science College, Kadakkal, Kollam, Kerala

Dr. T. Muthumanickam[2]
Professor & Head of Department of ECE, VMKV Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu

ABSTRACT:- IoT play increasing role impacting different fields such as smart transport, energy, cities, and healthcare applications . Today, the spread of many small devices forces publicizing the internet of things (IoT). In fact, IoT devices are manufactured by large number of companies and are being used for important and critical objectives. In other words, the most important advantage of Internet of Things (IoT) is achieving full communication between heterogeneous devices, heterogeneous networks and heterogeneous processing bandwidths. Thus, if the IoT can't merge the multimedia in an organized way, it will not be able to benefit from multimedia-based services and applications. In other words, involving multimedia in IoT is an important research direction that will develop new architectures, protocols as well as scenarios such as adapting security in health monitoring environment.

INTRODUCTION

As sensor networks and cloud computation technologies have rapidly developed over recent years, many services and applications integrating these technologies into daily life have come together as an Internet of Things (IoT). IoT aims to create connectivity for ''everything'' with minimum storage and computational capability. The IoT creates value-added information by comprehensively analyzing the state and location of two or more things. The application of IoT has been widely implemented in every sector such as security systems, industry, farming, and medicine. Among these services, in particular, the IoT oriented healthcare support system is one of the most promising and important directions for development and therefore, becomes a major focus of government and industry.

IoT based Health monitoring deploys machine learning and other data mining models, including Semantic Web technology to analyze and identify the status of a patient's condition and recommend cautions or alarm an immediate medical care. IoT has a lot of issues. Security is one of the major issue in the development of IoT and has to be dealt with effectively to make IoT a fruitful reality.

In a healthcare monitoring system, health data is shared by various health units. Every unit must provide data privacy because healthcare data includes essential information. All the world's attackers want to capture the health data. Therefore, the privacy of data must be protected. Cryptography proves to be a promising solution for a security problem. Implementation of conventional cryptography on resource-constrained sensor devices aggravates the security

challenges and demands for lightweight cryptography techniques which reduce the computational overhead without bargaining on the security.

In summary, IoT based Health monitoring extracts health signals from wearable devices and other various datasets, extracts relevant features, and builds personalized health predictive models for its subscribers and authorized researchers/doctors.

RELATED WORK

Ruidong Li *et al.* suggested a distributed authentication and authorization scheme (DAAS), where the Identity-Based Signature (IBS) was used to achieve distributed verifications on the identities of Publishers and Users and the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was used to enable the distributed and fine-grained authorization. DAAS has three phases, initialization, secure data publication, and secure data retrieval, which seamlessly integrate authentication and authorization with the Interest/Data communication paradigm in Information-Centric Networking (ICN). In an experimental evaluation, the suggested DAAS achieved lower bandwidth cost compared to the existing systems.

Norah Alassaf *et al.* presented a light-weight-cryptography algorithm based on SIMON in IoT driven setup. The approach also suggested further improvement to implement the original SIMON cryptography in order to reduce the encryption time and maintain the practical trade-off between security and performance. The method was compared with the Advanced Encryption Standard (AES) and the original SIMON block cipher algorithms in terms of execution time and memory consumption. The results corroborated that the approach was suitable for securing data in an IoT driven setup.

Priyan Malarvizhi Kumar *et al.* recommended scalable three-tier architecture to store and process a huge volume of wearable sensor data. Tier-1 focused on the collection of data from IoT wearable sensor devices. Tier-2 used Apache HBase for storing the large volume of wearable IoT sensor data in cloud computing. In addition, Tier-3 used Apache Mahout was used for developing the logistic regression-based prediction model for heart diseases. Finally, Receiver Operating Characteristic (ROC) analysis was performed to identify the most significant clinical parameters to get heart disease.

Haomiao Yang *et al.* presented an efficient privacy-preserving authentication scheme with adaptive key evolution, which can prevent illegal access to the patient's vital signs. Furthermore, the approach considered the leakage process of the key information to set proper key renewal interval, which could adaptively control the key evolution to balance the trade-off between the communication efficiency and security level. The performance evaluation proved that the scheme was computationally efficient for the typical mobile phone with limited resources, and it has low communication overhead.

Prosanta Gope and Tzonelih Hwang recommended a secure IoT based healthcare system using Body Sensor Network (BSN), called BSN-Care, which efficiently accomplish those requirements. The approach divided the security requirements into two parts: network security, and data security. Network security comprises authentication, anonymity, and secure localization. On the other hand, data security includes data privacy, data integrity, and data freshness. For enhancing the security, the approach used the lightweight anonymous authentication protocol. Finally, the experimental evaluation proved the security of the method.

Chia-Hui Liu and Yu-Fang Chung presented a user authentication scheme and data transmission mechanism that facilitates security and privacy protection, enable medical personnel to instantly monitor the health conditions of care receivers, and provide care receivers

with prompt and comprehensive medical care. Based on the smart cards and passwords, the scheme grants only legal medical personnel access to patient information such as body temperature, heart rate, and blood pressure. In addition, a secure cryptosystem was applied for establishing a data transmission mechanism. The security analysis verified that the system resists common attacks such as impersonation attacks, replay attacks, online and offline password guessing attacks, and stolen-verifier attacks.

PROBLEM STATEMENT

The existing research methods have some problems as listed below,

1. The Existing logistic regression model can no longer be trained. This is because the weight for the feature would not converge since the optimal weight would be infinite.
2. The existing classification technique has low Prediction Accuracy and it takes high computation time.
3. Authentication, trustworthiness, and privacy are the major challenges to turn IoT into a reality. The absence of authentication will collapse the sensor data, which will outweigh the benefit of IoT components.

PROPOSED METHODOLOGY

The IoT (Internet of Things) is an emerging technological revolution in future computing. Healthcare applications are considered as promising fields for wireless sensor networks, where the patients can be monitored using wireless medical sensor networks (WMSNs). Presently, hospitals are using these applications in order to access a patient's health data. Therefore, the cost for a user's identity management is increased as well as the authentication was decreased. The existing works presented the authentication scheme for the healthcare sector, but they provide low security. To overcome these issues, in this paper, a framework is developed for the authenticated transmission of the data from Wireless Body Sensor Networks (WBSN) in an IoT environment. Initially, the sensors present in the human body collect data from the human body signals. This data is sent to the cloud through a gateway. It is an efficient secure authentication scheme for a personalized healthcare system using wireless medical sensor networks.

Our proposed work starts with IoT sensor values of the patients. IoT devices continuously sense values like temperature, heartbeat, etc. from patients and send them to the Patients healthcare application through the Zigbee device. Here, the patients with IoT devices are located in a patient's house or some other place.

CONCLUSION

IoT technology is in its starting face but it have potential to impact human healthcare and associated market at a massive scale. The application of IoT has been widely implemented in every sector such as security systems, industry, farming, and medicine. Among these services, in particular, the IoT oriented healthcare support system is one of the most promising and important directions for development and therefore, becomes a major focus of government and industry.

REFERENCES

1. Yong-Yuan Deng, Chin-Ling Chen, Woei-Jiunn Tsaur, Yung-Wen Tang, and Jung-Hsuan Chen, "Internet of things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system", Sensors, vol. 17, no. 12, pp. 2919, 2017.

2. Geeta Sharma, and Sheetal Kalra "A lightweight user authentication scheme for cloud-IoT based healthcare services", Iranian Journal of Science and Technology, Transactions of Electrical Engineering, vol. 43, no. 1, pp. 619-636, 2019.

3. Jeannette Chin, Vic Callaghan, and Somaya Ben Allouch, "The internet-of-things: reflections on the past, present and future from a user-centered and smart environment perspective", Journal of Ambient Intelligence and Smart Environments, vol. 11, no. 1, pp. 45-69, 2019.

4. Davin Bagas Adriano and Wahyu Apsari Ciptoning Budi, "Iot-based integrated home security and monitoring system", In Journal of Physics: Conference Series, vol. 1140, no. 1, pp. 012006, 2018.

5. Jia-Li Hou, and Kuo-Hui Yeh, "Novel authentication schemes for IoT based healthcare systems", International Journal of Distributed Sensor Networks, vol. 11, no. 11, pp. 183659, 2015.

6. Santhiya K, Kamalakannan B, Muthu gowtham S, Pandian A, Ram pradeep R, "Human body sensor health monitoring system in the fusion of Iot and cloud computing", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), vol 5, no. 3, 2018.

7. Aaditya Jain, and Bhupendra Kumar Soni, "Secure modern healthcare system based on internet of things and secret sharing of IoT healthcare data", International Journal of Advanced Networking and Applications, vol. 8, no. 6, pp. 3283, 2017.

8. Cansu Eken, and Hanim Eken, "Security threats and recommendation in IoT healthcare", In Proceedings of The 9th EUROSIM Congress on Modelling and Simulation, EUROSIM 2016, The 57th SIMS Conference on Simulation and Modelling SIMS 2016, no. 142, pp. 369-374, 2018.

9. Prabhu M, Seethalakshmi G and Gollapudi Anisha, "Secured healthcare system in IoT", International Journal of Pure and Applied Mathematics, vol. 118, no. 20, pp. 3239-3244, 2018.

10. Sridar V, Revanesh. M, "Blended cryptography for secured data transfer in medical IoT devices", Future Technologies Conference (FTC), pp. 29-30, 2017.

11. Ruidongz Li, Hitoshi Asaeda, Jie Li, and Xiaoming Fu, "A distributed authentication and authorization scheme for in-network big data sharing", Digital Communications and Networks, vol. 3, no. 4, pp. 226-235, 2017.

12. Norah Alassaf, Adnan Gutub, Shabir A. Parah, and Manal Al Ghamdi, "Enhancing speed of SIMON: a light-weight-cryptographic algorithm for IoT applications", Multimedia Tools and Applications, pp. 1-25, 2018.

13. Priyan Malarvizhi Kumar, and Usha Devi Gandhi, "A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases", Computers & Electrical Engineering, vol. 65, pp. 222-235, 2018.

14. Haomiao Yang, Hyunsung Kim, and Kambombo Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system", Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1059-1069, 2015.

15. Prosanta Gope and Tzonelih Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network", IEEE Sensors Journal, vol. 16, no. 5, pp. 1368-1376, 2015.

16. Chia-Hui Liu, and Yu-Fang Chung, "Secure user authentication scheme for wireless healthcare sensor networks", Computers & Electrical Engineering, vol. 59, pp. 250-261, 2017.