INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Multi-level Authentication for Internet of Things to Establish Secure Healthcare Network –A Review

Shilpa Kansal
Department of CSE
Punjabi University Regional Centre for Information Technology and Management,
Mohali, Punjab, India
kansal.shilpa91@gmail.com

Navpreet Kaur
Department of CSE
Punjabi University Regional Centre for Information Technology and Management,
Mohali, Punjab, India
navpreetk.@gmail.com

Abstract— ***The Cloud based healthcare monitoring sensor networks (C-HMSN) consist of a number of wireless nodes connected to each other using wireless connections. As these wireless nodes are connected to base stations so they are highly prone areas for hacking attacks. During data analysis there is need to secure cryptographic keys when the HMSN nodes are in working condition, for secure propagation of the sensitive information. An Efficient corporate key management and distribution scheme is required to maintain the data security in HMSNs. Existing cryptographic key management and distribution technique usually consume higher amount of energy and put larger computational overheads on Wireless Sensor Nodes. The cryptographic keys are used on different levels of HMSN communication i.e. neighbour nodes, cluster heads and base stations. In this paper we will present a corporate improved key management architecture, called SECURE KEY EXCHANGE adaptable for the HMSNs, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. It allows only authorized applications to use the keys and administrator can remotely issue authenticated commands and verify system output. In addition, it also has to be improved to work with HMSN nodes, which means it must use less computational power of the HMSN. The wireless sensor node should be energy efficient, increasing the life of wireless sensor network.***

Keywords— Authentication, IoT security, Multi-level security in IoT, HMSN, Secure key exchange.

I. INTRODUCTION

Internet of Things refers to automation of all things around us. In other words it means without man to man or man to computer interaction, we can communicate or transfer data with the help of internet directly through the wireless mediums. Each and every object or people around us, are these days dependent on internet starting from the morning schedule till the late night sleep. Using such technology means that person can easily interact with the devices which are quite difficult and time consuming, by accessing it remotely. Use of IoT devices can access, record and analyse new data faster and accurately by reducing time and cost. IoT devices have sensory capabilities as they have been assigned an IP address through which they are connected with a network.

The main goal of IoT is to have smart world with smart- energy, health, building, transport, industry, city, home, family. The applications of internet go vaster in fields like mobile, telemedicine, agriculture automation, building management, security, travelling, pet monitoring, retail, transportation ,automotive ,every day things (like automobile refrigerator, smart watches, television, printer) and many more.

IOT devices in healthcare are of great importance. Various health monitoring devices are available like wearable heart monitors ,blood pressure ,sensor node, pulse oximetry sensor nodes, ECG sensor node, body area aggregator are available .Such devices gives bio feedback immediately, as when records is passed through healthcare server then the record is checked by the physician after passing through network. IoT devices in healthcare upraises the quality of patients care with high level of accuracy , As it offers right care, at right time ,by minimising the cost of care to a greater extent. Such devices help doctors to keep check on patients health on their smart phones about patients current status, or even if they are discharged from the hospitals. There are various monitoring devices for blood glucose level, pulse rate, blood pressure, ECG patterns, heart rate, and respiration rate.

With the use of more IoT devices, their Security has become one of the major key concerns for our personal privacy and public safety. Security fundamentals - authentication/ identification, confidentiality, integrity, non-repudiation need to be maintained. With the larger transfer of sensitive data over IoT devices there is more risk of data to been leaked, falsification, manipulation or IP theft to occur. Major security attacks can be steeling information , disruption of services like pacemakers , remote hacking of vehicle control system, personal fitness devices tells hacker were we are, locked door can be unlocked remotely. IoT devices suffer from cyber attacks thus resisting its security/ threat of cyber theft and financial transactions. Attack on unprotected devices, flaws in encryption, access control, brute force attacks leads to insecurity.

Iot devices and sensor equipped edge devices on a wired or wireless network sends data through gateway to a public or private cloud .So there is need to maintain encryption, data access control ,firmware updates ,data retention and privacy ,device physical and network vurnelabilies. Offloading the security into the network should be at its peak.

In the field of Cloud based healthcare monitoring sensor networks (C-HMSN), wireless body sensor network play a vital role. It’s a network of various wearable or implanted electronic devices that provide doctors the real time data about patients anywhere within or outside the medical center as that is made available online. These networks are composed of wireless sensor nodes (WSN’s) that transmit their ID or sensor data to the gateway. The network of sensors is kept on or close to the surface of patients body or may even plated into the tissue so that patients physiological data can be achieved regardless of patients location, his continuously. Sensors can be transceivers or receivers depending on the bandwidth of data to be collected. These sensors require accuracy, low power of signal processing and wireless capabilities and must be robust against various interferences in environment. WBAN’s are used for measuring glucose level in blood, insulin level, heartbeat, blood pressure. Halter device which is used for constant monitoring of heart or respiration rate. It constantly record and observe cardio vascular system. It’s also known as ambulatory ECG (electro cardiography) monitor. Electroencephalography or electrophysiological (EEG) is a test for detecting electrical activities of brain as it helps in diagnosing abnormalities, infections, tumors and the brain disorders. These networks aims in improving the quality of patient’s life at low cost and power, and high reliable sensor system. Helps in understanding the disease and response to treatment accordingly.

Healthcare database collects patient’s data, records clinical data, gives access and then retrieves on cloud. These database like Online Transaction Processing Database (OLTP), Medline, Health star, Toxline are quick and allows real-time transactional processing by reducing manual effort .Healthcare Database helps doctors and nurses by replacing paper work and preventing data loss.

II. LITERATUTE SURVEY

Hernandez-Rasmos, Jose L. et. al. [1] in this paper author proposed authentication and authorization scheme that is Deffie Hellman along with advanced encryption standard (AES) for the security of IoT sensor devices which is integrated with security framework Architectural Reference Model (ARM).

Kumar, Adarsh et. al.[2] has worked upon simulation and analysis of authentication protocols for mobile Internet of Things (MIoT). This work purposes authentication protocol for MIoT named single bar circular topology which helps in constructing a secure network for authenticating mobile devices. Radio frequency identification (RFID) based devices communicate with each other using various routing protocols. As in this zone routing protocol which is modelled using alloy model proved as the best for constructing a secure network with limited delay.

Abomhara, Mohamed et. al.[3] has given the study on security and privacy in the Internet of Things: Current status and open issues. It a study paper in which survey of current vision of IoT that is to attain its target which is to smarten the world and to overcome various challenges and difficulties that IoT is still facing. Various challenging aspects of IoT devices are as security and privacy issues such as authentication authorization of entities are introduced, design of architecture standards, categorizing IoT technologies

Ali, Syed Taha et. al. [4] has worked on the authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. In this paper the author introduces low cost and robust authentication scheme for healthcare monitoring devices .Develops optimizing framework to maximize data verification for given overhead and loss environment. Validates the scheme by verifying maximum percent of data can be authenticated with low overheads and at low cost.

Al Ameen, M. et. at. [5] Presents a secure Cloud-based Mobile Healthcare Framework using Wireless Body Area Networks (WBANs).Worked on storing the electronic medical records on cloud and providing security in Inter-Sensor Communication.

Lee, Jun-Ya et. al.[6] has proposed a lightweight authentication protocol for internet of things. For the security and privacy of IoT objects an encryption scheme is purposed which is based on binary operations known as XOR manipulation thus eliminating the use of hash functions flaws in RFID protocols thereby enhancing the security.

Finally summary with potential features is generated.

AUTHORS & YEAR OF PUBLICATION	**PAPER TITLE**	**PROPOSED WORK**	**MERITS**	**DEMERITS**
Hernandez-Ramos, Marcin Piotr Pawlowski, Antonio J. Jara, Antonio F. Skarmeta, and Latif Ladid. *IEEE ,2015*[1]	Toward a Lightweight Authentication and Authorization Framework for Smart Objects	In this paper, the aim of the authors has been focused at the development of the lightweight authentication mechanisms for the IoT sensor devices. The authors have utilized the Diffie-Hellman authentication protocol along with the AES encryption for the security of the internet of things (IoT).	Diffie-Hellman is a fast authentication scheme. AES is robust encryption method.	AES is still vulnerable to the various types of brute force attacks. Diffie-Hellman is highly exposed algorithm. There are several successful and quick break into mechanisms that are available for Diffie-Hellman.
Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal *IEEE Journal, 2014* [2]	Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT).	In this paper, the single bar circular topology based authentication method has been proposed for MIoT. This protocol helps in authenticating the mobile devices for constructing secure network. The proposed protocol is modelled using Alloy model. The proposed model has been named as the Zone Routing Protocol (ZRP) and proved best from the experimental results as the best protocol for constructing a secure network.	Based on Zone Routing which empowers the local connectivity. Has been considered secure.	-NA- Note: The routing mechanism can be used for the proposed IoT model.
Abomhara, Mohamed, and Geir M. Koien *IEEE , 2014*[3]	Security and privacy in the Internet of Things: Current status and open issues.	This paper has been published as the survey of the threats and security techniques. In this paper, the IoT vision, existing security threats, and open challenges in the domain of IoT are discussed. The current state of research on IoT security requirements is discussed and future research directions with respect to IoT security and privacy are presented.	Have considered many threats over the internet of things. The open challenges has been deeply described and evaluated in this paper.	The authentication schemes have not been evaluated clearly. The paper does not describe any scheme as the best one.

Ali, S. T., Sivaraman, V., & Ostry, D. *Elsevier,2014* [4]	Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring.	In this paper the authors have proposed, analysed, and validated a practical, lightweight robust authentication scheme suitable for health-monitoring. They have developed an authentication scheme that is both low-cost, and loss-resilient. They have designed a framework for optimizing placement of network coding within the tree to maximize data verifiability for a given overhead and loss environment.	The work has been described on the internet of things connectivity. The scheme has been made suitable specifically to the health care monitoring networks.	Does to include any data encryption or authentication model to secure the link between the patient and the healthcare database.
Al Ameen, M., Liu, J., & Kwak, K. *Springer , 2010* [5]	Security and privacy issues in wireless sensor networks for healthcare applications.	Presents a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs).Presents two folds: first, it attempts to secure the inter-sensor communication by multi-biometric based key generation scheme in WBANs second, the electronic medical records (EMRs) are securely stored in the hospital community cloud and privacy of the patients' data is preserved. The evaluation and analysis shows that the proposed multi-biometric based mechanism provides significant security measures due to its highly efficient key generation mechanism.	Proposes the secure cloud based WBANs. The EMR has been properly secured in this scheme.	Key generation scheme is computationally costly. The transmission delay can be reduced by using the lightweight but secure algorithm.
Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang *IEEE Transactions, 2014*[6]	A lightweight authentication protocol for internet of things.	In this paper, the authors have proposed an encryption method based on XOR manipulation, instead of complex encryption such as using the hash function, for anti-counterfeiting and privacy protection. The enhancement of the security is described and hardware design methodology is also demonstrated.	This scheme is considered fast. Can authenticate various nodes at once quickly.	The XOR manipulation is highly vulnerable to several encryption break-into methods. Hence not applicable to sensitive networks.

III. RESEARCH GAPS

- AES cryptographic schemes have been found prone to the brute force attacks or the cryptanalysis attacks and also AES is slower encryption scheme.
- The use of diffie-hellman scheme also makes it insecure due to its higher level of public exposure as well as the less complexity

in the key generation and verification policy.

- The IoT devices does not handle the automatic data sharing cooperation between the IoT server and the IoT device, hence it is not resilient against the connectivity breakage.
- The performance of the proposed key exchange is slightly better than the existing schemes in some cases (performance parameters like computational cost, etc.), where it is under performed or almost similar in the case of probability of key exposure, which does not show the significant improve in the results.
- Everything about the key exchange scheme, which includes the key-table generation, key verification, etc. are being provided by the IoT server, which may be hacked during the data exchange.

These drawbacks can be mitigated using our proposed scheme. The new cooperative hybrid IoT architecture data privacy protection scheme is aimed at development of a resilient scheme against time-based and location-based mobile attacks.

The next section describes the conclusion.

CONCLUSIONS

We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds. Meanwhile, we have discussed important concepts related to their sharing and integration in healthcare clouds and analysed the arising security and privacy issues in access and management of electronic health records. Then we present a security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an electronic health record cloud. Finally, we illustrate the development of the proposed electronic health record security reference model through a use-case scenario and describe the corresponding security countermeasures and possible security techniques. In this paper, we establish the urgent need for research in user data privacy in the cloud, and outline the risks of not achieving it. We have proposed the preventive rather than detective approaches to increasing accountability. Preventive approach in the proposed model is based on key exchange model for the user data privacy, integrity and data confidentiality. Also the proposed method is capable to protect against the security breach attacks on the healthcare databases. The results have proved the effectiveness of the proposed solution.

In future, we will enhance the proposed model to work more efficiently and quicker. The approach would be enhanced to protect against many types of attacks with one security solution. Also the elapsed time will be improved to increase the speed of the proposed approach.

REFERENCES

[1] Hernandez-Romas , Jose L. ,Marcin Piotr Pawlowski ,Antonio J. Jara ,Antonio F. Skarmeta , and latif Ladid. " Towars a Lighweight Authentication and Authorization Framework for Smart Objects." *Selected Areas in communications, IEEE Journal on 33*, vol. 4, pp. 690-702, IEEE 2015.

[2] Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal, "Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT)", in *Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on*, pp.423-428: IEEE, 2014.

[3] Abomhara, Mohamed, and Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues." in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, pp. 1-8: IEEE, 2014.

[4] Ali S. T., Sivaraman, V.and Ostry, D. "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring." in *Future Generation Computer Systems*, vol. 35,pp. 80-90, ELSEVIER,June 2014.

[5] Al Ameen,Liu J.,Kwak K. " Security and Privacy Issues in Wireless Sensor Neworks for Healthcare Applications." in *Journal of Medical Systems,*vol. 36,pp. 93-101,SPRINGER,Feb. 2010.

[6] Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang. "A lightweight authentication protocol for internet of things." in *Next-Generation Electronics (ISNE), 2014 International Symposium on*, pp. 1-2: IEEE, 2014.