Data Privacy In Healthcare Networks With Secure Key Exchange Mechanism

MADHU[1], ER.AMANDEEP KAUR[2]

[1] *M.Tech Student At Chandigarh Engineering College Landran Mohali,Punjab,India*
[2] *Assistant Professor At Chandigarh Engineering College Landran Mohali,Punjab,India.*

Abstract - *The adoption of digital patients record,increased regulation,provider consolidation and the increasing need for information exchange between patients and doctors,all point towards the need for better information security. Traditionally, health monitoring was performed with regular check basis, where the patient must remember its symptoms; the doctor checks patients on regular or after a fixed period and formulates a diagnostic, then monitors patient progress along the treatment, if possible. Home healthcare becomes mandatory for diseases like Parkinson or Alzheimer, providing memory enhancement through medicine reminders, mental stimulation through sounds or images of object's location.This review paper compares important techniques with each other in terms of encryption comparative study between two such widely used encryption algorithms(AES) and (RSA) and Congestion control mechanisms.*

Key Words: **Information security,privacy,healthcare information system,research literature, electronic healthcare.**

1.INTRODUCTION Healthcare monitoring is the most important issue, as it involves the quality of life a given individual can have.It is and will be better to prevent an illness than to treat it, so individual monitoring is required as a periodic activity. The aging population of developed countries present a rise of government's budget, and presents new challenges to healthcare systems, namely with old age people living on independent senior housing. Traditionally, health monitoring was performed on regular check basis, where the patient must remember its symptoms; the doctor performs some check and plan a diagnostic, then monitors patient progress with the treatment, if possible. However, some symptoms only manifest themselves in daily activities, where an individual may feel some pain or discomfort. Healthcare applications of wireless sensor networks allowed in-home assistance, smart nursing homes, clinical trial and research augmentation. In-home healthcare becomes mandatory for diseases like Parkinson or Alzheimer, providing memory enhancement through medicine reminders, mental stimulation through sounds or images of object's location, control over home appliances, medical data lookup, and emergency situation.

2.LITERATURE SURVEY

- **ALI GHAFFARI .** Authors have worked upon Congestion control is deemed to be one of the most significant challenges in Wireless Sensor Networks which is attributed to resource constraint specification and the number of deployed nodes.
- **ZONGWEI ZHOU.**proposed KEY IT SIMPLE AND SECURE which is a key management algorithm.He presents a new key management architecture, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. This protects the entire life cycle of cryptography keys. It allows only authorized applications and/or users to use the keys.
- **IVAN DAMGARD**. proposed "A secure key management method for cloud environments." Authors have studied the levels of security on the basis what they can and what they cannot obtain in the security models.And after studying that all,Authors have proposed light-weight protocols achieving maximal security and report on their practical performance.

- **RAMASWAMY CHANDRAMOULI**. worked on " **Cryptography Key Management Issues & Challenges in Cloud Services.** An analysis of the common state of practice of the cryptography operations that provide those security capabilities reveals that the management of cryptography keys takes on an additional complexity in cloud environments compared to enterprise IT environments **.**

- **MACRO TILOCA .** proposed, that wireless sensor networks are used in many applications including industrial apllications. In such apllications time division access is used for data communication among sensor nodes. However, Time division-based wireless sensor networks are particularly prone to Selective Jamming attack, a specific form of Denial of Service attack .In this, he present a self-adaptive and decentralized Medium access control-layer solution against selective jamming in time division-based wireless sensor network.
- **SEAL SARKAR . (2012)** Proposed "Protocol for Energy-Efficient Routing in Self-Organized Module" introduced an energy consumption model through which energy of all sensor nodes can be calculated. Also the author adopted a trust module based energy efficient routing protocol. Trust module is used to calculate the value of routing metric. Experiments would be conducted to compare the proposed protocol on the basis of routing overhead. This comparison shows that it increases ratio of delivery of packets and uses less energy.

3.PREVIOUS SYSTEM

In today's era, body sensors are being used at a large to check the patients in their routine activity treatment. Body sensors which are wearable to patients body are used to send data to the medical databases directly through the wireless mediums (cellular networks, wireless network,etc.).The patient are informed by the medical database centers about their health after fixed intervals by sending reports to their home or on their emails.The healthcare monitoring data is aggregated on the servers and various types of algorithms are used for the healthcare data analysis. The user privacy becomes the major concern in such healthcare monitoring systems.The authentication scheme based healthcare data privacy algorithm in the base paper has been proposed. The existing authentication scheme is based on secure key exchange. In the existing system, they have not focused upon bandwidth allocation and Quality of service .In this research, we are trying to solve the problem of confidentiality and data integrity by adding up various security protocols and algorithms with the existing authentication based on healthcare monitoring systems.

4. PROPOSED MODEL

The proposed algorithm for user data privacy in healthcare monitoring system will be a combination of data compression, encryption and authentication schemes. The new hybrid user privacy model will ensure the security level hardening for the secure data transfers in the healthcare monitoring systems. The confidentiality of the user sending the data will be achieved by using the secure key exchange between the healthcare sensors and medical database. The secure key exchange model will be update in the proposed model than the existing user privacy solution. The key table for proposed scheme will use randomized mathematical key generation functions. The key table sharing will be performed in the neighbor building state of the security model. To take on the data integrity, the encryption algorithm will be used. The encryption algorithm will ensure the privacy of the user data by making the data unreadable during data transmissions between the medical databases and healthcare sensors. In this proposed model we also have focused upon bandwidth allocation.

5. CONCLUSIONS

Cryptography is the method for providing security mechanisms. Cryptography is usually known to as "the study of secret", which is most attached to the definition of encryption.Encryption is the process of translating, vanilla text i.e. "readable" form to "non readable" for providing security against different attacks. This paper provided a comparative study between two such widely used encryption algorithms **AES(Advanced Encryption Standard)** and **RSA(Rivest ,Shamir & Adleman)** on the basis of their ability to check security and data protection against attacks and speed of encryption and decryption.The algorithm which use only one key for encryption and decryption are known as Symmetric algorithms also known as private key algorithms and the algorithm which use different keys for encryption and decryption are known as Asymmetric algorithms or public key algorithm.

6. REFERENCES

[1] Ali, S. T., Sivaraman, V., & Ostry, D. (2014). Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. Future Generation Computer Systems, 35, 80-90.

[2] Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, 36(1), 93-101.

[3] Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks. Procedia Computer Science, 34, 511-517

[4] Kumbhare, M. A., & Chaudhari, M. M. (2014). IDS: Survey on Intrusion Detection System in Cloud Computing.

[5] Peng, X., Zhang, H., & Liu, J. (2014). An ECG Compressed Sensing Method of Low Power Body Area Network. TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(1), 292-303.

[6] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. (2008, April). EKG-based key agreement in body sensor networks. In INFOCOM Workshops 2008, IEEE (pp. 1-6). IEEE

[7] Wan, J., Zou, C., Ullah, S., Lai, C. F., Zhou, M., & Wang, X. (2013). Cloud-enabled wireless body area networks for pervasive healthcare. IEEE Network,27(5), 56-61.

[8] Wang, H., Peng, D., Wang, W., Sharif, H., Chen, H. H., & Khoynezhad, A. (2010). Resource-aware secure ECG healthcare monitoring through body sensor networks. Wireless Communications, IEEE, 17(1), 12-19.