INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue5)

Available online at: www.ijariit.com

Security Enhancement of the Telemedicine and Remote Health Monitoring Models

Nishu Dhiman[1], Tejpal Sharma[2]

Chandigarh Group of Colleges,

dhimannishu.4@gmail.com[1], cgccoe.csetejpal@gmail.com[2]

ABSTRACT—the telemedicine applications are the application utilized for the remote monitoring and health assessment of the people living in the remote areas. The networks of the doctors and the field executives utilizes the various kinds of the healthcare sensors for the health checkup of the people by collecting and transmitting over the internet for the treatment of the affected ones. The information being propagated through the internet between the healthcare sensors and the online server model is always prone to the several forms o the attacks. In this paper, the proposed model has been designed to improve the level of security over the telemedicine network. The proposed model will be improved by using the robust encryption with the highly scrambled authentication key. The performance of the proposed model will be assessed under the various performance parameters which define the network health as well as the security level.

KEYWORDS—Robust authentication, Telemedicine security, highly scrambled authentication data, Paired key based authentication.

I. INTRODUCTION

The technological advancements in wireless communication and electronics have resulted in an exceedingly growing interest within the field of wireless detector networks. [1] A detector network involves deploying the array of sensors for distributed watching of real time events. The detector networks have restricted energy, because the detector nodes require the battery for the electronic operations. The detector nodes even have restricted memory and machine capability and might be deployed in remote areas or inhospitable piece of ground. There has been the increasing use of detector networks always important applications cherish watching patients in hospitals and military applications. These applications create it necessary to possess an honest security infrastructure for detector networks. The readying of those networks in military applications and therefore the restricted power and memory, create the look of a security protocol terribly difficult.

The security of Wireless detector Networks (WSN) will be compromised in many ways. A distant user accessing base station info will be prevented from doing thus in an exceedingly sort of ways in which. Communication between the bottom station and detector nodes will be blocked. This will be accomplished by analog attack based network jamming of signals or by digital jamming within the style of Denial of Service attacks that flood the network, base stations or each. In our own way of breaching security is to destroy the bottom station itself. This will be accomplished by watching the amount and direction of packet traffic toward the bottom station in order that the placement is eventually disclosed. Eavesdropping will be wont to track and deduce the placement of the bottom station for destruction. There are numerous alternative ways to breach the WSN security.

Several attacks are sometimes caused as a result of the shortage of security within the detector node lay communications. Parenthetically, a hacker will simply create a reference to the insecure wireless detector nodes to infect or jam the complete detector network. These forms of attacks will be reduced or stopped by exploitation key exchange schemes that exchange the secure cryptography based scrambled keys between the nodes to make sure the safety of communications.

During the periods once the WSN nodes are in performing the operations and applications under the various conditions, they have secure cryptography based scrambled keys for secure propagation of the sensitive info. Economical key management and distribution theme play a crucial role for the information security in the sensor networks. Existing cryptography based scrambled key

management and distribution technique sometimes consume higher quantity of energy and place larger machine overheads on Wireless detector Nodes. The cryptography based scrambled keys are used on completely different communication levels of WSN communications i.e. Neighboring nodes, major units as the cluster heads and base transceiver stations. An efficient company key management and distribution policy is needed to keep up the safety of the wireless detector networks. [6]

II. LITERATURE SURVEY

Ramaswamy Chandramouli et. Al. (2013) have worked on cryptography based scrambled key management problems & challenges in cloud services. The critical analysis of the common state of the application of the cryptography based scrambled operations that offer those security capabilities reveals that the management of cryptography based scrambled keys takes on an extra quality in cloud environments compared to enterprise IT environments. Ivan Damgård et. al. (2013) has projected a secure key management technique for cloud environments. Authors have studied the degree of security on the idea what they will and what they can't acquire within the security models. And when finding out that each one, authors have projected a light-weight protocols achieving peak security, and report on their sensible performance.

N. Suganthi et. Al. (2014) have projected the critical algorithmic program to support the institution of 3 styles of keys for every device node, a personal key shared with the bottom station, a combine wise key shared with neighbor device node, and a gaggle key that's shared by all the nodes within the network. The algorithmic program used for establishing and change these keys are under the energy efficient algorithm by using the smart energy consumption mechanism and minimizes the involvement of the bottom station. Zongwei Chow dynasty et. Al. (2013) has projected a brand new key management system named KISS within which the matter of fine-grained key usage management and secure system administration are resolved. Kiss aims at reducing price by hoping on hardware and minimizes the system TCB by creating the utilization of thin- hypervisor-based style and light-weight administrator devices.

Md. Monzur Morshed et. Al. (2013) have projected cluster primarily based secure routing protocol (CBSRP) may be the MANET routing protocol that ensures secure key management and communication between mobile nodes. It uses Digital Signature and a technique Hashing technique for secure communication. Consistent with CBSRP, it forms a gaggle of tiny clusters incorporates 4-5 nodes and afterward the communication takes place between mobile nodes. Marco Tiloca et. al. (2013) has projected wireless device networks are presently utilized in several application situations, as well as industrial applications and manufactory automation. In such situations, Time Division Multiple Access (TDMA) is often used for electronic communication among device nodes. Fagen Li et. Al. (2016) projected a theme that permits a sender within the certificate-less cryptography surroundings to transmit a message to a receiver in identity primarily based cryptography surroundings .As compared with existing schemes ,the machine price during this theme is reduced by concerning twenty second and fifty three .and energy consumption is reduced by concerning thirty third and fifty four. Ravi Kishore Kodali et. Al. (2014) proposes a key management technique, with its reduced resource overheads, that is extremely suited to be utilized in gradable WSN applications. Each sensor node identities primarily based key management (PBK) and probabilistic key pre-distribution schemes are created use of at completely different gradable levels. The projected key management technique has been enforced mistreatment IRIS WSN nodes.

III. PROBLEM FORMULATION

In today's world, body sensors are being employed at an oversized to observe the patients in their routine activity post- or pre-treatment. Wearable body sensors or alternative wireless sensors sometimes sends information to the medical databases directly through the wireless mediums (cellular networks, Wi-Fi, Zigbee, etc.). The patients are educated by the medical info centers concerning their health on weekly or monthly basis by causation reports to their home or on their emails. The WSN information is aggregative on the servers and numerous kinds of algorithms are used for the aid information analysis. The user privacy becomes the foremost concern in such WSN systems. The authentication theme based mostly aid information privacy algorithmic rule within the base paper has been projected. The present authentication theme relies on secure key exchange supported diffie-hellman key exchange algorithmic rule. The diffie-hellman algorithmic rule has its share of drawbacks as well as the actual fact that there are valuable exponential operations concerned, and also the algorithmic rule can't be wont to write messages - it is used for establishing a secret key solely. There's additionally an absence of authentication. During this analysis, we tend to are planning to solve the matter of confidentiality and information integrity by mitigating the protection threats caused by the shortcomings of the present diffie-hellman key exchange theme within the existing IoT based mostly WSN system by adding up numerous security protocols and algorithms with the present authentication supported WSN systems. Within the existing system, the authentication is being done utilizing the Elliptic Curve Cryptography (ECC) theme based mostly key exchange agreements, the performance of the projected theme has been evaluated on the premise of comparison of key property at preparation, comparison of key exposure and procedure value.

IV. METHODOLOGY

At first stage, an in depth literature study would be conducted on the secure management ways or architectures. Additionally, the safety issues and demand analysis of key management in WSNs would be totally studied and developed. Literature study can lead US towards refinement the structure of the planned security resolution style. Afterwards, the planned resolutions are enforced in

MATLAB machine and an intensive performance analysis would be performed. Obtained results would be analyzed and compared with the present techniques. The diffie-hellman authentication mechanism uses the inter-key relationship based mostly key exchange between 2 ends, that makes it vulnerable to the estimate and recall attacks. The irregular key table generation with the inter-key relationship elimination technique is predicted to resolve the threat caused by the estimate and recall attacks. Therefore to beat the matter related to the diffie-hellman, the planned model is designed with the irregular key table generation with one-on-one key relationship for the aim of strong authentication to revitalize the amount of security. Our theme doesn't depend upon the key reversal or re-computational method, however is strong and rigid in nature, that doesn't permit any of the key estimate attacks. Such attacks don't let the sensing element device to become hostile to the hackers and don't expose any data to the hackers.

V. CONCLUSION

The robust security model is found to be required in the telemedicine networks, which are used for the various types of health monitoring applications. The proposed model design has been proposed in this research for the purpose of creating the secure telemedicine networks propagating the data over the internet. The proposed model design includes the robust encryption algorithm along with the robust paired authentication data to mitigate the data hijacking and cryptanalysis attacks. The proposed authentication algorithm is supposed to improve the level of security in the telemedicine data exchange over the telemedicine networks. The proposed solution performance will be monitored and evaluated under the multi-faceted security and performance analysis experiments.

REFERENCES

[1] Abdallah, Walid, Noureddine Boudriga, Daehee Kim, and Sunshin An. "An efficient and scalable key management mechanism for wireless sensor networks." In *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, pp. 687-692. IEEE, 2014.
[2] Kodali, kishore Ravi. "Key management technique for WSNs." In *Region 10 Symposium, 2014 IEEE*, pp. 540-545. IEEE, 2014.
[3] Varadarajan, Prabhakar, and Garth Crosby. "Implementing IPsec in Wireless Sensor Networks." In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on*, pp. 1-5. IEEE, 2014.
[4] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.
[5] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.
[6] Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[7] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.

[8] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", International Conference on Emerging Technology & Factory Automation (ETFA), vol. 18, pp. 1-8, IEEE, 2013.
[9] Md. Monzur Morshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", International Advance Computing Conference (IACC), vol. 3, pp. 571-576, IEEE, 2013.

