ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Computing for Wireless Medical Sensor Data by Using Bloom Filter Technique

Mr. Firas Tarik Jasim Alkhzraji
Master of Science in Computer Science,
Mahatma Gandhi College, (Affiliated to Acharya Nagarjuna University),
N.G.O Colony Road, Guntur-522006, Andhra Pradesh, India.

ABSTRAC:

In recent years, wireless sensor networks have been widely used in healthcare applications, such as hospital and home patient monitoring. Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. A lot of work has been done to secure wireless medical sensor networks. The existing solutions can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data. In this paper, we propose a practical approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy.

1. INTRODUCTION:

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.[1] Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored in hospitals and even at home using wireless medical sensor networks (WMSNs).

In recent years, many healthcare applications using WSNs have been developed, such as CodeBlue. Alarm-Net, UbiMon, MEDiSN, and MobiCare. A typical example of healthcare application with WSNs is Alarm-Net developed in University of Virginia for assisted-living and residential monitoring. Alarm-Net is composed of mobile body network, emplaced sensor network, AlarmGate applications, backend systems, and user interfaces as follows: Mobile body network has wireless sensor devices worn by a patient which provide physiological sensing. Data from the mobile body network is transmitted through the emplaced sensors to user interfaces or back-end systems.[2] Emplaced sensor network has devices deployed in the living space to sense environmental quality or conditions, such as temperature, dust, motion, and light. Emplaced sensors maintain connections with mobile body networks as they move through the living space.

AlarmGate applications serve asapplication-level gateways between the wireless sensor networks and IP networks. These nodes allow user interfaces and a connection to a back-end database for long-term storage of data. Back-end systems provide online analysis of sensor data and long-term storage of data. User interfaces allow any legitimate user of the system to query sensor data. Wireless medical sensor networks certainly improve patient's quality-of-care without disturbing their comfort. However, there exist many potential security threats to the patient sensitive physiological data transmitted over the public channels and stored in the back-end systems.[3]

Cite this article as: Mr.Firas Tarik Jasim Alkhzraji, "Secure Computing for Wireless Medical Sensor Data by Using Bloom Filter Technique", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6, Issue 2, 2019, Page 38-43.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Typical security threats to healthcare applications with WSNs can be summarized as follows. Eavesdropping is a security threat to the patient data privacy. An eavesdropper, having a powerful receiver antenna, may be able to capture the patient data from the medical sensors and therefore knows the patient's health condition. He may even post the patient's health condition on social network, which can pose a serious threat to patient privacy. Impersonation is a security threat to the patient data authenticity. In a home care application, an attacker may impersonate a wireless rely point while patient data is transmitting to the remote location. This may lead to false alarms to remote sites and an emergency team could start a rescue operation for a non-existent person. This can even defeat the purpose of wireless healthcare. Modification is a security threat to the patient data integrity.[4]

OBJECTIVE OF THE PROJECT

In recent years, wireless sensor networks have been widely used in healthcare applications, such as hospital and home patient monitoring. Wireless medical sensor networks are more vulnerable to eavesdropping, modification, impersonation and replaying attacks than the wired networks. A lot of work has been done to secure wireless medical sensor networks. The existing solutions can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data. In this paper, we propose a practical approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy

2. LITERATURE REVIEW

A Novel Security and Privacy Protection for Wireless Medical Sensor Data

We propose a practical approach to prevent the inside attack by using multiple data servers to store patient data. The main influence of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' confidentiality. Healthcare applications are considered promising fields for WMSNs, where patients can be monitored. Transmission in wireless environment needs safety and privacy of medical data. To keep the privacy of the patient data, a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g., physician) to access the patient data, we proposed an access control protocol, where three data servers cooperate to provide theuser with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher) to perform statistical analysis on the patient data, we proposed some new protocols for average, correlation, variance and regression analysis, where the three data server cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results.[5]

Sharemind: a framework for fast privacy-preserving computations

Gathering and processing sensitive data is a difficult task. In fact, there is no common recipe for building the necessary information systems. In this pa-per, we present a provably secure and efficient general-purpose computation system to address this problem. Our solution—SHAREMIND—is a virtual machine for privacy-preserving data processing that relies on share computing techniques. This is a standard way for securely evaluating functions in a multi-party computation environment. The novelty of our solution is in the choice of the secret sharing scheme and the design of the protocol suite. We have made many practical decisions to make large-scale share computing feasible in practice. The protocols of SHAREMIND are information-theoretically secure in the honest-but-curious model with three computing participants. Although the honest-but-curious model does not tolerate malicious participants, it still provides significantly increased privacy preservation when compared to standard centralized databases.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However, the current implementation has several restrictions; most notably it can use only three computing parties and can deal with just one semi-honest adversary. Hence the main direction for future research is relaxing these restrictions by developing computational primitives for more than threeparties. We will also need to study the possibilities for providing security guarantees against active adversaries. Another aspect needing further improvement is the application programmer's interface. A compiler from a higher-level language to our current assembly-like instruction set is definitely needed. Implementing and benchmarking a broad range of existing datamining algorithms will remain the subject for further development as well.[6][7]

3. SYSTEM ANALYSIS

Existing System

Wireless medical sensor networks certainly improve patient's quality-of-care without disturbing their comfort. However, there exist many potential security threats to the patient sensitive physiological data transmitted over the public channels and stored in the back-end systems. Typical security threats to healthcare applications with WSNs can be as follows. Eavesdropping is a security threat to the patient data privacy. An eavesdropper, having a powerful receiver antenna, may be able to capture the patient data from the medical sensors and therefore knows the patient's health condition. He may even post the patient's health condition on social network, which can pose a serious threat to patient privacy. Impersonation is a security threat to the patient data authenticity. In a home care application, an attacker may impersonate a wireless rely point while patient data is transmitting to the remote location. This may lead to false alarms to remote sites and anemergency team could start a rescue operation for a non-existent person. This can even defeat the purpose of wireless healthcare. Modification is a security threat to the patient data integrity. While the patient data is transmitted to the physician, an adversary may capture the physiological data from the wireless channels and alter the physiological data. After the attacked data (i.e., altered data) is sent to the physician, it could endanger the patient Data breach is a security threat to the patient data privacy. A data breach is an incident in which sensitive, protected or confidential patient data has potentially been viewed, stolen or used by an individual unauthorized to do so. For example, a malicious patient database administrator may use the patient data (such as, patient identity) for their personal benefit, such as for medical fraud, fraudulent insurance claims, and sometimes this may even pose life threatening risks.

Disadvantages of Existing System:

1. The solutions can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data.

Proposed System

We further improve the security of the solution given by Yi et al. Like, we assume that the wireless medical sensor network is composed of some medical sensors, three data servers, and some users. Each sensor sends the patient data to the three data server in the same way as. Unlike, the three data servers process the queries, such as statistical analysis on the patient data, from the users on the basis of the Paillier and ElGamal cryptosystems instead of the Share mind system. The patient data privacy can be preserved as long as atleast one of three data servers is not compromised. Even if two data servers are compromised but one data server is not compromised, our solution is still secure.

Advantages of Proposed System:

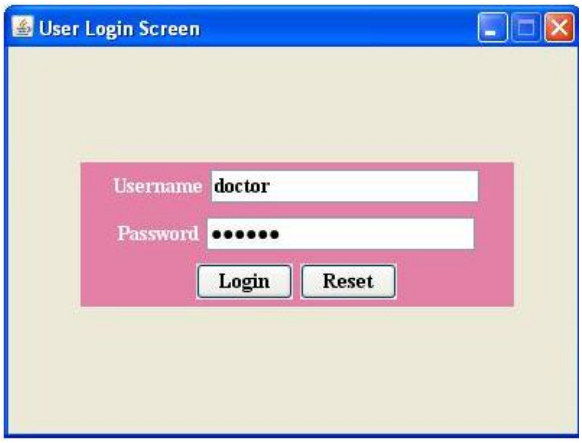
1. Most of current solutions focus on how to protect the wireless medical sensor networks against the outside attacks, where the attacker does not know any information about the secret keys.
2. We propose a new data access protocol on the basis of the Paillier cryptosystem. The protocol allows the user (e.g., physician) to access the patient data without revealing it to any data server.

4. OUTPUT SCREENS:

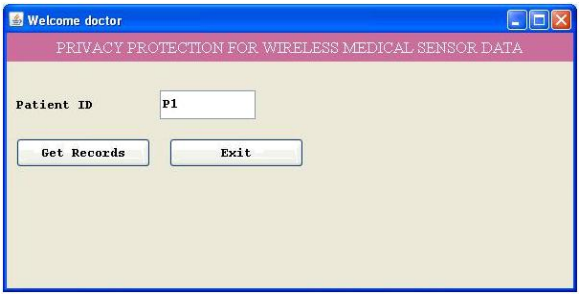
To show the output step by step

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

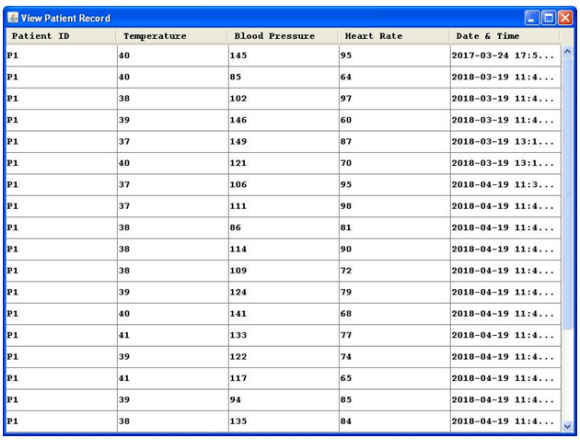
In above screen click on 'User Access' button to get below screen.



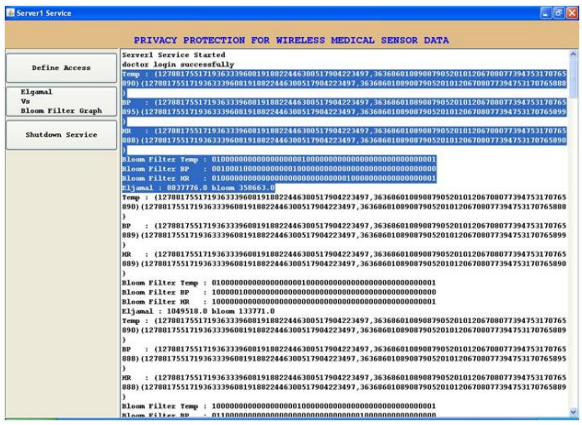
In above screen login as doctor to get below screen, this username will be given by admin in server1 screen.



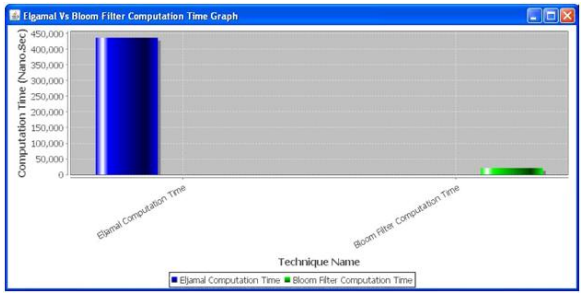
In above screen enter patient id to get below screen records.



Above screen records which are coming from servers are in encrypted format.



See below server screen.



In above screen selected text you can see temperature, BP and HR (heart rate) are in encryption format with both techniques eljamal and bloom filter. We can see computation time for both techniques in bottom line and eljamal time is more than Bloom filter time. Now click on 'Elgamal Vs Bloom Filter Graph' button to see computation time in graph. In above screen x-axis represents technique name and y-axis represents computation time in nano seconds for those techniques.

5. EXTENSION

In this project to secure patient data author is using Mac code and elJamal encryption which is little bit put heavy computation on sensors and we can use bloom filter encryption technique as extension which can reduce computation time compare to elJamal and Mac code . A Bloom filter is a space-efficient probabilistic data structure, conceived by Burton Howard Bloom in 1970, that is used to test whether an element is a member of a set. False positive matches are possible, but false negatives are not – in other words, a query returns either "possibly in set" or "definitely not in

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

set". Elements can be added to the set, but not removed (though this can be addressed with a "counting" filter); the more elements that are added to the set, the larger the probability of false positives. Bloom proposed the technique for applications where the amount of source data would require an impractically large amount of memory if "conventional" error-free hashing techniques were applied. In other words a Bloom filter is a simple spaceefficient randomized data structure for representing a set in order to support membership queries. Bloom filters allow false positives but the space savings often outweigh this drawback when the probability of an error is controlled. Bloom filters have been used in database applications since the 1970s, but only in recent years have they become popular in the networking literature. The aim of this paper is to survey the ways in which Bloom filters have been used and modified in a variety of network problems, with the aim of providing a unified mathematical and practical framework for understanding them and stimulating their use in future applications.

ADVANTAGE OF BLOOM FILTER

Bloom filters have a strong space advantage over other data structures for representing sets, such as self-balancing binary search trees, tries, hash tables, or simple arrays or linked lists of the entries. Most of these require storing at least the data items themselves, which can require anywhere from a small number of bits, for small integers, to an arbitrary number of bits, such as for strings (tries are an exception, since they can share storage between elements with equal prefixes). Linked structures incur an additional linear space overhead for pointers. A Bloom filter with 1% error and an optimal value of k, on the other hand, requires only about 9.6 bits per element — regardless of the size of the elements. This advantage comes partly from its compactness, inherited from arrays, and partly from its probabilistic nature. If a 1% false positive rate seems too high, each time we add about 4.8 bits per element we decrease it by ten times.

Bloom filter

A Bloom filter is a space-efficient probabilistic information organization with the purpose of is used to experiment whether a component is a part of a set. The price we pay for efficiency is that it is probabilistic in nature that means, there might be some False Positive results. False tremendous matches are viable; however false negatives are not – in different words, a query returns both "likely in set" or "actually not in set". Elements may be delivered to the set, however now not eliminated (even though this could be addressed with a "counting" clear out); the more factors which are delivered to the set, the bigger the chance of fake positives.[8][9]

6. CONCLUSION

In this paper, we have investigated the security and privacy issues in the medical sensor data collection, storage and queries and presented a complete solution for privacy reserving medical sensor network. To secure the communication between medical sensors and data servers, we used the lightweight encryption scheme and MAC generation scheme based on SHA-3 proposed. To keep the privacy of the patient data, we proposed a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g., physician) to access the patient data, we proposed an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher)to perform statistical analysis on the patient data, we proposed some new protocols for average, correlation, variance and regression analysis, where the three data servers cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results. Security and privacy analysis has shown that our protocols are secure against both outside and inside attacks as long as one data server is not compromised.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Performance analysis has shown that our protocols are practical as well. In this paper we introduced the new notion of Bloom filter encryption (BFE) as a variant of puncturable encryption which tolerates a non-negligible correctness error. We presented various BFKEM constructions. The first one is a simple and very efficient construction which builds upon ideas known

BILIOGRAPHY:

[1] P. Belsis and G. Pantziou, "A k-anonymity privacy-preservingapproach in wireless medical monitoring environments," J. Personal Ubiquitous Comput., vol. 18, no. 1, pp. 61–74, 2014.

[2] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur.Symp. Res. Comput. Security, 2008, pp. 192–206.

[3] R. Chakravorty, "A programmable service architecture for mobilemedical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput.Commun. Workshop, Pisa, Italy, Mar. 13–17, 2006, pp. 532–536.

[4] Crypto++ 5.6.0 Benchmarks [Online]. Available: http://www.cryptopp.com/benchmarks.html, 2009.

[5] J. Daemen, G. Bertoni, M. Peeters, and G. V. Assche. (2012, Jul. 6).Permutation-basedencryption, authenticationand authenticatedencryption. Proc. Directions Authenticated Ciphers, Stockholm, Sweden [Online].

[6] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, and N. Challa,"Real-Time and secure wireless health monitoring," Int. J. Telemed.Appl., pp. 1–10, Jan. 2008.

[7] W. Diffie and M. Hellman, "New directions in cryptography,"IEEE Trans.Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[8] (2013, Jul.). Digital signature standard (DSS). FIPS PUB 186-4[Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[9] T. ElGamal, "A public-key cryptosystem and a signature schemebased on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31,no. 4, pp. 469– 472, Jul. 1985.