Attribute-Based Authentication System Using SHA-2 for m-Health Care Applications

[1]Krishnaveni S, [2]B.Jothi Sundari, [3]SivamohanS

Assistant Professor Software Engineering SRM University
Assistant Professor Information Technology SRM University
vanimithila@gmail.com, **jothi.sundari@gmail.com, sivamohan7@gmail.com**

Abstract -**New generic cryptanalytic techniques for hash function based on MD5 and SHA-1, along with the fact that the SHA-2 family of hash functions was designed with a similar structure. The security of such technology was been a challenge over years and a majority of attacks is based on guessing the distance of the rotation where data is located. To ensure the patient data security and integrity the healthcare providers need to implement strong digital security and encryption methods for user. To handle all emerging attacks and security challenges, algorithms have to be implemented to run a constant business continuity service in the field of health care. To ensure the confidentiality and security of electronic information (patient EMR, patient identifier, hospital medical records, etc.).This project is implementing using Java Platform as Frontend and Backend as HTML .SHA-2 algorithm provides a unique security framework which ensures full protection against web-services based attacks as well as vulnerability based IPS and DOS attacks from harming a healthcare providers applications. This project guarantees the availability of locally hosted and globally dispersed mission and patient applications services and data centers. To provide full protection against emerging attacks, it utilizes the latest security measures such as SHA-2 encryption algorithm .The SHA-2 algorithm is widely implemented in popular security applications and protocols like SSL, TLS , IPsec , S/MIME, SSH, PGP etc. There are many Crypto Currencies that rely on SHA-2 as a part of their Proof of work scheme.SHA-2 rightfully performs the most basic SHA function of effectively verifying the procedure of message authentication along with password verification as well.**

Keywords-Healthcare, Computing, Privacy Preserving, Secure Hash Algorithm, Mobile-Healthcare, Remote Healthcare.

1. INTRODUCTION

Today Medical world started to implement these are the problem causes are Denial of service attack, Timestamp, Data loss, Data integrity. These are existing problems in my base paper AES algorithm was used in existing mobile health care application ,system initialization the algorithm used is AES, as the algorithm cannot transmit the PHI data of a medical user who is in a critical situation.AES algorithm is not ready to encrypt and it takes a lot of time to be sent and occupies a large memory.MD5 algorithm was used in existing mobile health care application to ensure security of the medical user database ,but it has many implications some of them are, It's the less secure when compared to SHA -2.Message digest length bits exceeds 128bits.MD5 algorithm can prevent attacks to some extents only,MD5 can be access only in 32 bit machines.These are the problem identification are Existing technology of mobile healthcare application has a drawback due to security lapsing and time. So in my proposed work I have replaced AES & MD5 algorithm by SHA-2 algorithm. SHA provides 2^{160} bit operation to break the original encrypted message .It's more fast and robust.SHA-2 algorithm has proved that there is no internal attacks reported up to yet and so far.SHA-2 algorithm is more secure and send the bunches of data without time lapsing to the PHI.

2. RELATED WORK

We design a distributed authentication system in mHealth networks, where patients/physicians use their verifiable attributes to authenticate each other before communication. Our attribute-based authentication system is able to simultaneously provide the privacy protection and verifiability of patients/physicians' verified attributes. Based on different application scenarios, we provide progressive privacy levels corresponding to patients/physicians increasing privacy requirements during their interactions. Extensive simulations and experiments are conducted on different platforms to verify the performance of our schemes in terms of security, efficiency, and feasibility. This will ensure better privacy of the user medical data to be stored in PHI using SHA-2 algorithm. Instead of glucose meter device and application we are going to approach the IOT devices.

3. SECURITY REQUIREMENTS

Every wireless network with sensors or other devices handling critical information is vulnerable to many security breaches. This is especially true when there is a wireless transmission channel to be secured against various

attacks posed by malicious parties. The presence of patient health information records also needs to ensure the following security properties. Confidentiality makes sure that the information is understandable only to that person for whom it was meant. Integrity guarantees that no malicious alteration has been made to data while in transit or otherwise. Availability guarantees that data is handy to anyone who needs it at the right time. Authentication proves to the data receiver that it was indeed sent by the person who claimed to be the sender. Authorization guarantees that only those who are authorized to perform certain actions can perform them. Self-organization guarantees that the sensors are autonomous in handling sticky situations that arise in the network amongst them.

Non-repudiation makes sure that no one can deny that a message was received or sent by them. Privacy & anonymity guarantees that no one can be targeted based on their identity or location, which is prevented from exposure. Security Requirements and Assumptions Our main security objective is to preserve the privacy of each user's identity and attributes. First, we assume that a user's attribute set can uniquely identify a particular user, such that we cannot reveal user's attributes in plaintext form during the protocol run. Also, since users use credentials of attributes to authenticate each other, we require the credential of each attribute should be kept undisclosed. Second, our system should be secure under tracing attacks launched by adversaries, which means the information used for verification from the same user in different queries should remain indistinguishable. Otherwise, it is easy for an adversary, or even a benign user to trace one particular user. Besides, according to the restrictions and laws, like the Health Insurance Portability and Accountability Act (HIPPA), we forbid physicians and hospitals to distribute PHRs to any unauthorized personnel. In terms of privacy concerns, patients use verified PHRs to communicate with physicians and/or patients without using real identities in order to avoid being traced.

4. ATTRIBUTE-BASED AUTHENTICATION

Without proper authentication anyone can access a patient's private data for malicious purposes. Authentication mechanisms are a necessary security measure to allow only authorized people access to data. Lu et al. in [8], discussed about a mobile healthcare social network in which elderly patients can communicate with other elderly patients with similar symptoms. In order to prevent other people from knowing their symptoms and to identify those with the same symptoms, they have proposed a secure same symptom-based handshake (SSH) scheme. In the scheme, every patient is provided with a pseudo-ID and a private key corresponding to his/her symptom. So, if two patients meet, if they have the same symptom, they can use their respective private keys to mutually authentication each other. The paper also explained about patient health information delivery through this connection among patients. Liang et al. proposed an attribute-oriented authentication scheme in [1]. They explained about a health social network in which the users are each assigned attributes based on certain characteristics by the attribute trusted authority. Each of the HSN users have the ability to generate an attribute proof for themselves, whereby the sensitive attributes can be anonymized if they so choose. Only by verifying the provided attribute proof (figure 2), will the other users be able to know what attributes an HSN user has and thus can authenticate themselves to access others' personal medical data. Recently, D. He et al. proposed an authentication protocol for wireless medical sensor networks. It helps to authenticate the health professional in order to access a patient's physiological data. The protocol in [7] consists of professional registration and patient registration phases, followed by the login and authentication phase. The authentication is performed by inserting a smart card in a card reader, which inputs the professional's id and password, followed by using random numbers and checking timestamps for authenticating. This protocol provides user anonymity as well. Althobaiti et al.'s [17] is an example of a biometric trait being used for authentication in wireless sensor network. They used the iris of the user to regenerate the user's key every time the user needs be authenticated which considerably enhances the security. After extracting the iris's features, the biometric encryption is performed by using a fuzzy commitment scheme, the biometric data is then stabilised. This stabilised data is bound with the user's random generated key during registration phase. The saved hash value of the encryption key is used during the remote authentication process.

ATTRIBUTE	JUSTIFICATION	PRIORITY
Security	System security is empowered by SHA-2 algorithm with its multiple variants and its size of n.	High
Availability	The data source needed to implement the measure is available and accessible within the timeframe for measurement. The costs of abstracting and collecting data are justified by the potential for improvement in healthcare applications	High
Performance	Performance gain and achieve over 50% improvements on both End user satisfaction and Health service provider.	High

5. PROPOSED SYTEM

The software should be active by 24/7 to monitor the user health. Mobile application should be aware of receiving data from wearable (sensor) devices.IOT Device should convert messages into PHI data format which is readable by Trust Authority. Network should be uninterrupted and easy to communicate with cloud server by all time. The software security should be guaranteed by proposing algorithm for PHI data, which is accessible by user & Trust Authority. These are the requirements Analysis are Users need IOT Device as a wearable healthcare device which mobile can communicate through Bluetooth. User should have Smartphone supported by Android or IOS mobile operating system in which user can install M-healthcare application. User need 3G network connection to upload the PHI to cloud server which is trustable network communication such as Airtel, Aircel, Vodafone, Etc.,PHI data should be secured bySHA-2 which preserves the privacy of user PHI stored on cloud server. We first give a brief overview to our proposed system. Our main design goal is to establish an authentication system in mHealth networks, which leverages the verifiable.

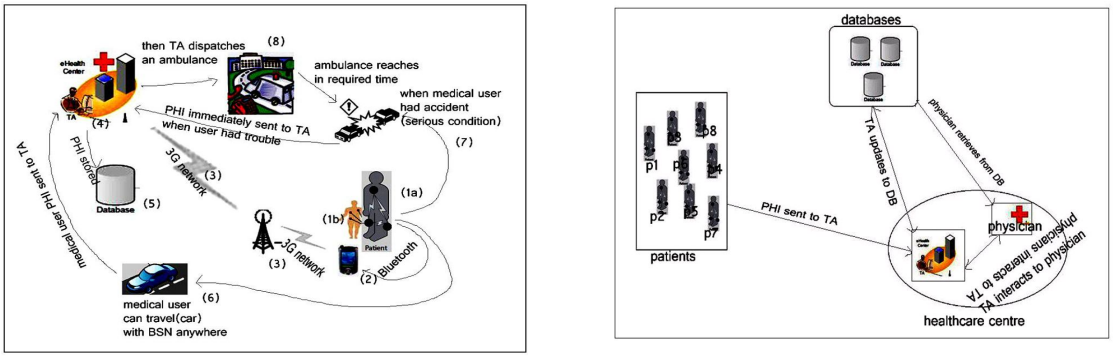

Figure 1: Architecture of Attribute-Based Authentication System For m-Health Care Applications

6. CONCLUSION

In this paper, we propose a framework of attribute-based authentication system in mHealth networks. Our framework applies the no interactive proof system as the basic building block, and we give formal definitions of four progressive privacy levels. The attribute-based authentication schemes designed for higher privacy levels preserve more stringent privacy on attributes and attribute values, but cost more computation and communication resources. Based on the security analysis, we show that our scheme meets both the verifiability and privacy of attributes and attribute values. According to extensive theoretical and experimental results, we show the efficiency and feasibility of our proposed scheme under different privacy requirements.

7. REFERENCES

[1].A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 2009.

[2] R.Lu,X. Lin, X. Liang, and X. Shen, "Secure Handshake with Symptoms-Matching: The Essential to the Success of Mhealthcare Social Network," Proc. Fifth Int□l Conf. Body Area Networks (BodyNets □10),

[3] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Trans. Parallel and Distributed System, to be published.

[6] M.R. Yuce, S.W.P. Ng, N.L. Myo, J.Y. Khan, and W. Liu, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for m-Healthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011

[8] [Online]. Available: http://www.healthegift.com/page/50

[9] [Online]. Available: http://www.nytimes.com/2011/11/05/us/u cla-health-system-warns-about-stolen-records.html

[10] Ponemon Institute. (2012). Third Annual Survey on Medical Identity Theft [Online]. Available: http://www.ponemon.org/

[11] [Online]. Available: http://healthcaremgt.net/blog/2011/08/areyou-educating-patients-on-ehr/

[12] D. Zismer, J. McCullough, and P. Person, "Integrated health care economics. Part 2: Understanding the revenue drivers in fully integrated community health systems," Physician Exec., vol. 35, no. 4, pp. 26–28, 2011.

[13] A. Moumtzoglou and A. Kastania, E-Health Systems Quality and Reliability: Models and Standards. Hershey, PA, USA: IGI Global, 2010.

[14] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Proc. SECURECOMM, Singapore, 2010, pp. 89–106.