Enhanced Remote Health Monitoring System with Secure and Privacy Preserving Authentication Services

Arathi G, Ashwin Kumar M

Abstract— Nowadays Mobile Phones or Smartphones are mainly used for communications and updating knowledge purposes, (i.e., voice calling, video calling, chatting with friends, relatives, browsing for news updates and so on). Mobile Phones or Smart Phones are not only used for Communications and also useful in many ways by using applications like healthcare monitoring, location finder, chatting applications, travelling applications and so on. With the help of wireless body sensor networks (BSN), healthcare monitoring application helps to monitor the health condition of medical users regularly with the help of health care centre. With the help of smart phones, a mobile healthcare application extends the operations of healthcare provider for enhanced health monitoring for patient. A mobile healthcare emergency service plays an important role but the data communication and privacy revelation is still a problem. However, the flourish of Mobile-Healthcare is still facing many challenges. Our proposed scheme aims to address the problems in the securities and privacy issues in Mobile-Healthcare emergency. The data is collected by the mobile phone and is transferred to the health care centre database in the encrypted format and a digital signature will be created and appended along with this encrypted data for authentication, integrity, confidentiality etc. Using the hash algorithm named Hash Round Function Algorithm and the self-certified public key system, a new kind of digital signature algorithm named Hash Round Function and Self-certified public key system Digital Signature Algorithm is used. The signature is verified by the trusted authority before taking any action on data. Finally, the users analyze the H-S DSA from two aspects of security and time-complexity. And, the results show that the new designed digital signature algorithm named H-S DSA not only has better security strength, but also has lower time- complexity and the information is more secure.

Index Terms— Authentication services, Digital signature, Emergency system, Hash Round Function Algorithm, Mobile computing, Mobile health care, Self certified public key system.

1 INTRODUCTION

Mobile computing is a human – computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Mobile software deals with the characteristics and requirements of mobile applications. All smart phones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart phones that can come from means of communication like SMS, MMS, wifinetworks and GSM. Mobile devices like Smart phone, tablet PCs, etc., are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate high experience of various services from mobile applications which run on the devices and/or on remote servers via wireless networks.

The rapid progress of Mobile Computing (MC) becomes a powerful trend in the development of IT technology . However, the mobile devices are facing many challenges in their resources and communications. The limited resources significantly slow down the improvement of service qualities. Mobile healthcare largely discussed the use of mobile communication and other latest technologies that are integrated in the mobile. The main aim of the mobile healthcare is to monitor the medical users remotely and inform them their pdiagnosis report through mobile as sms or as e-mail and also to react quickly to their life threatening situations and thereby saving lives. Now a day's most of the patients using home monitoring service for diagnosing, no longer needed to monitor in hospital surroundings (Toninelli et al , 2009).

In this proposed work, security in the network environment is focused. M-healthcare service is provided with security and privacy. They are different medical users, they have different sensitive diseases like heart attack, emergency situation like meet with accidents etc, they need automatic help from any of the emergency centre. Figure.1. shows the overall architectural design of the proposed Emergency Healthcare Monitoring system. The Figure depicts that the centralized Healthcare Station or centre has been integrated with the Smartphone users, specialized doctors through the internet. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

- *Arathi G is currently pursuing masters degree program in computer science and engineering in Mangalore institute of technology and engineering,VTU University, Karnataka, India, E-mail: sreearathi@mail.com*
- *Ashwin Kumar M is the senior assistant professor in the department of computer science and engineering, Mangalore institute of technology and engineering, Mangalore, Karnataka, India. E-mail: ashwin@mite.ac.in*

The system also has an alert mechanism for emergency cases. This alert mechanism helps to point out the emergency cases to the healthcare professionals.

2 Related Works

In [1], With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high-reliable-PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

Advances in wireless networks [5], sensors, and portable devices offer unique chances to deliver novel anytime anywhere medical services and information, thus enabling a wide range of healthcare applications, from mobile telemedicine to remote patient monitoring, from location based medical services to emergency response. Mobile e-health has great potential to extend enterprise hospital services beyond traditional boundaries, but faces many organizational and technological challenges. In pervasive healthcare environments, characterized by user/service mobility, device heterogeneity, and wide deployment scale, a crucial issue is to discover available healthcare services taking into account the dynamic operational and environmental context of patient-healthcare operator interactions. In particular, novel discovery solutions should support interoperability in healthcare service descriptions and ensure security during the discovery process by making services discoverable by authorized users only. This article proposes a semantic-based secure discovery framework for mobile healthcare enterprise networks that exploits semantic metadata (profiles and policies) to allow flexible and secure service search/retrieval. As a key feature, our approach integrates access control functionalities within the discovery framework to provide users with filtered views on available services based on service access requirements and user security credentials.

In our aging society, m-Healthcare social network [8] (MHSN) built upon wireless body sensor network (WBSN) and mobile communications provides a promising platform for the seniors who have the same symptom to exchange their experiences, give mutual support and inspiration to each other, and help forwarding their health information wirelessly to a related health centre. However, there exist many challenging security issues in MHSN such as how to securely identify a senior who has the same symptom, how to prevent others who don't have the symptom from knowing someone's symptom? In this paper, to tackle these challenging security issues, we propose a secure same-symptom-based handshake (SSH) scheme, and apply the provable security technique to demonstrate its security in the random oracle model. In addition, we discuss a promising application -- social-based patient health information (PHI) collaborative reporting in MHSN, and conduct extensive simulations to evaluate its efficiency in terms of PHI reporting delay.

Patient monitoring provides [11] flexible and powerful patient surveillance through wearable devices at anytime and anywhere. The increasing feasibility and convenience of mobile healthcare has already introduced several significant challenges for healthcare providers, policy makers, hospitals, and patients. A major challenge is to provide round-the-clock healthcare services to those patients who require it via wearable wireless medical devices. Furthermore, many patients have privacy concerns when it comes to releasing their personal information over open wireless channels. As a consequence, one of the most important and challenging issues that healthcare providers must deal with is how to secure the personal information of patients and to eliminate their privacy concerns. In this article we present several techniques that can be used to monitor patients effectively and enhance the functionality of telemedicine systems, and discuss how current secure strategies can impede the attacks faced by wireless communications in healthcare systems and improve the security of mobile healthcare.

Personal health record (PHR) [15] is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by

exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

Wireless body sensor network [10] hardware has been designed and implemented based on MICS (Medical Implant Communication Service) band. The MICS band offers the advantage of miniaturized electronic devices that can either be used as an implanted node or as an external node. In this work, the prototype system uses temperature and pulse rate sensors on nodes. The sensor node can transmit data over the air to a remote central control unit (CCU) for further processing, monitoring and storage. The developed system offers medical staff to obtain patient's physiological data on demand basis via the Internet.

Data mining can [3] extract important knowledge from large data collections—but sometimes these collections are split among various parties. Privacy concerns may prevent the parties from directly sharing the data and some types of information about the data. This paper addresses secure mining of association rules over horizontally partitioned data. The methods incorporate cryptographic techniques to minimize the information shared, while adding little overhead to the mining task.

3 Proposed Work

In this paper, we propose a new enhanced secure and privacy-preserving mobile health monitoring system. With the help of smart phones, a mobile healthcare application extends the operations of healthcare provider for enhanced health monitoring for medical users.

When a person wants the service of the healthcare centre, he or she has to register in health centre. A Trusted Authority (TA) will be assumed, who controls all the operations of the remote healthcare centre. TA will create a particular record for each medical user and keep it in a database. He will install software in the medical user's android phone which collects each users PHI data and send it to the TA in an encrypted form. TA will decrypt it and save it in the database and then it is examined by the medical professionals. These PHI data will be secured by appending cryptographic digital signature to it. A new digital signature algorithm known as H-S DSA is used. Digital signature will provide more security. Digital signature is essential in modern world to verify the sender's identity. SMS notifications are also included as a response to the users.The application in the medical users mobile uses a signing algorithm to sign the message. The message and signature will send to the TA. The receiver after receiving this combination applies a verifying algorithm on it. If the result is true, the message is accepted otherwise it is rejected. A digital signature needs a public-key system. The signer signs with his/her private key and the receiver verifies by using their public key. The digital signature will provide authentication, integrity, and non repudiation. Along with encryption digital signature is highly secure. The software developed for mobile allows the input of patient's health information from the equipment and then will send it to the health centre. The system must request username and password for access in the software as well as in the web part. Only after authentication system will allow access. Software must retrieve, update, and store data and allow the patients to view their medical record online also. The user can receive the diagnosis as the email in the address given at the time of registration, and can receive the report in SMS in the number given. The e-mail and the mobile number is verified for existence at the time of registration and if needed it can be altered later. Encryption and Digital signature appending is done in the medical users mobile phone .Decryption and the Digital signature verification are done by the TA in the health care centre.

4 Algorithm

Digital Signature Algorithms based on Public key cryptosystem, such as Diffie-Hellman RSA and ELGamal, are all algorithms where the signer uses the private key to generate the message's signature, and then the verifier uses the signer's public key to verify the signature. Generally speaking, public keys are all kept in the key directory maintained by the System Administrator. When verifying the digital signature, the verifier will first obtain the public key through public communication channel. There is a problem in this process, that is, a false public key is being substitute for a true public key. If the adversary replaces some legitimate users' public keys in key directory by public keys corresponding to the private keys he choose, or he replaces the public keys in its transmission process, he will be able to fake any of those users' signature, which are the so-called active attacks and fake attacks. Most of the existing digital signature schemes have this problem. In order to overcome this shortcoming, it is necessary to verify the validity of public key firstly before using the public key to verify signatures. For this a new digital signature algorithm named H-S DSA (Hash Round Function and Self-Certified Public Key System Digital Signature Algorithm), using HRFA algorithm and the above Self-certified public key method.

4.1 Self Certified Public Key System

Self-certified public key system (SCPKS) was proposed by Girault in 1991, which was commonly called RSA-based SCPKS, because the public/private key pair of this system is based on RSA cryptography. It consists of two steps including system initiation and user registration. In system initiation, System Administration (SA) will choose two prime number p, q, calculate N=p.q, and get the integral number g (maximum exponent number in (Z/N^Z)). Then calculate the secret key according to RSA, with regards that $(e, d) \equiv 1 \pmod{\varphi(N)}$ be satisfied (φ is Euler's constant). And make public N, g, e whereas p, q, d would be kept confidential. In user registration When user U_i with an identity ID_i wants to access the system, the user should first choose a key x_i in $(Z/NZ)^*$ and calculate

$$V_i = g^{-x_i} \bmod N \quad (1)$$

Then send $\{ID_i, v_i\}$ to SA to register. His public key would be then calculated by SA using eq (1).

$$y_i = (v_i - ID_i)^d \bmod N \quad (2)$$

Conclusion from eq.(1) and eq.(2): the public key of user U_i is actually the signature of his key and ID, which is produced by SA. Meanwhile, the private key of user is unknown to SA. User U_i can then verify the validity of public key y_i using eq (3):

$$y_i^e + ID_i = g^{-x_i} \bmod N \quad (3)$$

The self-certification procedure of public key is:

If user U_i wants to verify his identity, these steps based on Beth's or Schnorr's authentication protocol need to be executed. User U_i sends $\{ID_i, v_i\}$ to the verifier, who would then calculate using eq (4)

$$V_i = (y_i^e + ID_i) \bmod N \quad (4)$$

U_i chooses a random number r_1 , and calculates t_1 using eq (5) and send it to the verifier.

$$t_i = g^{r_i} \bmod N \quad (5)$$

Verifier would choose a random number k in (Z/N^z), and send it to U_i .U_i calculates s_i using eq. (6), and send it to the verifier.

$$s_i = r_i + x_i .k \quad (6)$$

Verifier verifies the eq (7)

$$g^{x_i} .v_i^k = t_i \bmod N. \quad (7)$$

Then, if eq (7) is tenable, verifier would consider the identity of U_i valid, otherwise invalid. Based on the analysis above, no extra the public key y_i is self-certified. Under FAC and DL, however, except for U_i, x_i cannot be derived from y_i or any other public information. In the event that SA forges a U_i , saying he chooses a private key x_i , calculates the corresponding public key y_i using eq (2) and manages to pass the verifying equation of eq (3), the fact that one user U_i has two valid public key would however certificate the dishonesty of SA.

4.2 Hash Round Function and Self Certified Public Key System Digital Signature Algorithm

Self-certified public key can effectively overcome active attacks and fake attacks, so on this basis, the digital signature algorithm similar to ELGamal (H-S DSA) is presented. H-S DSA consists of four steps: system initiation, user registration, signature creation and signature verification. The first two steps are the same as that of Girault's SCPKS. What is different is that SA needs to make public a one-way hash round function h during system initiation with the output length shorter than that of N, that is for any m, we have $|h(m)| \le |N|$. The main purpose of h is to condense the coming signature message into message abstract so as to avoid plaintext attack. In the case of signature creation, M is a message that needs to be signed. The signer U_i chooses a random number w_i, and calculates the signature (r_i, s_i) of M, where we have

$$r_i = g^{w_i} \bmod N \quad (8)$$

$$s_i = w_i + x_i .h(M, r_i) \quad (9)$$

Afterwards, U_i sends M and the signature (r_i, s_i) to the verifier. After receiving M and (r_i, s_i), verifier will verify eq. (10):

$$g^{s_i} \times (y_i^e + ID_i)^{h(M, r_i)} = r_i \bmod N \quad (10)$$

If eq (10) is tenable, the verifier accepts the signature validity of M, otherwise it will deny.

5 Algorithm Analysis

To ensure that an algorithm meets or exceeds the designed expectations, it is essential to analyze the performance of this algorithm to detect potential problems, this process is called as Algorithm Performance Analysis. Specific to the H-S DSA, its performance analysis including security analysis and time complexity analysis, is to check whether the algorithm can work effectively.

In the case of security analysis, H-S DSA argorithm has used a one-way hash function, and its safety mainly lies in the hash round function used in each round. In addition to the one-way hash function, the safety of H-S DSA also depends on the following two well-known password assumptions: Facts Factorization Hypotheses (FAH) and Discrete Logarithm Problem (DLP).

In the FAH, If N is the product of two large prime numbers, and two integers e and d satisfy: $e.d=1 \pmod{\varphi(N)}$, then the three items that will not be feasible in the calculation are find the factors of N, give integers M and C to find d which makes $C^d = M \pmod N$, give integer C to find M which makes $M^e = C \pmod N$. In DLP, Give a large prime number p, and g is the primitive element over GF (p). Integer $y \in (1, p-1)$ is not feasible in the calculation of finding out x to make $y = g^x \bmod p$. Next, on the basis of Facts Factorization Hypotheses and Discrete Logarithm Problem, we analyze the three possible attacks to H-S DSA. These attacks include exposing a secret parameter, forging of digital signature of given information.

Attack 1: Adversary discloses the user's secret key x_i via U_i 's public key y_i .

Security analysis: adversary could get $V_i = (y_i^e + ID_i) \bmod N$

from $y_i = (v_i - ID_i)^d \bmod N$ which implies that he may calculate x_i directly by $v_i = g^{-x_i} \bmod N$. $y + ID = g \bmod N$. However, in such situation, FAC and DL assumption are inevitable for him to face.

Attack 2: Adversary discloses user's secret key Xi from U_i 's signature to M, i.e. (r_i, s_i) .

Security analysis: suppose that adversary obtains W_i in advance, he could then calculate x_i from (10) even if only r_i is known to him. In other words, adversary can calculate w_i via (9), the same as that in attack 1, which means still that FAC and DL assumption would be still inevitable. Moreover, (3) could be another approach to X_i and w_i . However, the amount of unknown variables i x and i w is always larger than that of equations in system. This makes the attempt impossible.

4 Conclusion

In this paper, a secure and privacy preserving enhanced M-health care emergency system is proposed. We implement a new digital signature scheme called H-S DSA to prevent attacks. It provides authentication, integrity and confidentiality to the PHI data that is send from the medical user to the healthcare centre. The alert mechanism provided point out the emergency cases to the authority. H-S DSA not only has better security strength, but also has lower time- complexity and the information is more secure.

Acknowledgment

The First author is grateful to Mr. Ashwin kumar M for guiding and motivating in the progress of her master degree. Also express her sincere thanks to Mr. Udanesh N and Mangament of VTU University.

References

[1] Rongxing Lu, Member , IEEE, Xiaodong Lin, Senior Member, IEEE , and Xuemin (Sherman) Shen, Fellow , IEEE, "SPOC : A Secure and Privacy Preserving Opportunistic Framework for mobile healthcare

emergency", IEEE transactions on parallel and distributed systems, VOL. 24, NO. 3, MARCH 2013.

[2] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping for Ehealth Systems,"IEEE J. Selected Areas in Comm., vol. 27, no. 4, pp. 365-378, May 2009.

[3] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks,"IEEE Wireless Comm.,vol. 17, no. 1, pp. 51-58, Feb. 2010.

[4] J.Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems,"IEEE Trans. Parallel Distributed and Systems,vol. 21, no. 6, pp. 754-764, June 2010.

[5] "Exercise and Walking is Great for the Alzheimer's and Dementia Patient's Physical and Emotional Health," http://free-alzheimers-support.com/wordpress/2010/06/exercise-and-walking/, June 2010.

[6] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The Green, Reliability,and Security of Emerging Machine to MachineCommunications,"IEEE Comm. Magazine, vol. 49, no. 4, pp. 28-35, Apr. 2011.

[7] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing,"Proc. Ann. Int'l Conf. Cryptology Organized (CRYPTO '01), pp. 213-229, 2001.

[8] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for vehicular communications,"IEEE Trans. Vehicular Technology,vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[9] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.

[10] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,"IEEE Trans. Vehicular Technology, vol. 61, pp. 86-96, 2012.

[11] http://www.uaproperty.com/articles/In-Ukraine-ambulance-come-atient-10-minute s.html, 2012.

[12] S. Ross, Introduction to Probability Models, Ninth Ed.,2007 X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in Vanets," Proc. of INFOCOM '11, pp. 2147-2155, 2011
.

[13] W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data,"Proc. of CRPIT '14,ser. CRPIT '14, pp. 1-8, 2002.

[14] I. Ioannidis, A. Grama, and M. Atallah, "A Secure Protocol for Computing Dot-Products in Clustered and Distributed Environments,"Proc. of ICPP '02,pp. 379-384, 2002

[15] Rifat shahariyar, Md. Faizul bari, Gourab kundu, Sheikh Iqbal and Md. Musthafa Akbar, Bangladesh University of Engineering & Technology, University of Illinois at Urbana-Champaign, Marquette University : "Intelligent Mobile Health Monitoring System (IMHMS)" , International Journal of Control and Automation Vol.2, No.3, September 2009