Eleyon
SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY
Full Length Article

Privacy Preserving Wireless Medical Data on Cloud

Dr.R. Poonkuzhali[a], Devina B[b], Gomathi R[b], Sri Annalakshmi N[b]

[a]*Professor,Department of Information Technology,K.S.Rangasamy College of Technology*
[b]*Department of Information Technology, K.S.Rangasamy College of Technology*
[b]*Department of Information Technology, K.S.Rangasamy College of Technology*
[b]*Department of Information Technology, K.S.Rangasamy College of Technology*

***Corresponding Author**
Dr.R. Poonkuzhali

ABSTRACT: During the last few years, there is a great emergence of wireless medical sensor networks (WMSNs) in the healthcare industry. Wireless medical sensors are the cutting edge components for healthcare application and provide drastically improved quality-of-care without sacrificing patient comfort. The proposed scheme uses two-factor (i.e., password and smartcard) user authentication, where each user must prove their authenticity first and then access the patient vital signs. (Note: User and professional are used interchangeably and user or professional may be a doctor, a nurse, a surgeon or a technician. Also, it is believed that two-factor authentication provides strong and high level of security (i.e., secure access of individual physiological data from wireless sensors)

Keywords: Wireless Medical Sensor Networks(WMSN), Clould Service Providers(CSP)

1 Introduction

A wireless medical sensor network is a network that consists of lightweight devices with limited memory, low computation processing, low-battery power and low bandwidth . These medical sensors (e.g., ECG electrodes, pulse oxi-meter, blood pressure, and temperature sensors) are deployed on patient's body and collect the individual's physiological data and sends the collected data via a wireless channel to health professionals' hand-held devices (i.e., PDA, iPhone, laptop, etc.). A physician can use these medical sensor readings to gain a broader assessment of patient's health status. The patient's physiological data may include heartbeat rates, temperature, blood pressure, blood oxygen level, etc.

Wireless medical sensor technology has offered tremendous advantages to healthcare applications, such as continuous patient monitoring, mass-causality disaster monitoring, large-scale in-field medical monitoring, emergency response, etc. Further, these WMSNs provide many new ways for acute disease analysis (e.g., motion analysis for Parkinson's disease).However, wireless healthcare development has many challenges, such as reliable data transmission, fast event detection, timely delivery of data, power management, node computation and middleware. Further, patients' security and privacy is one of the big concerns for healthcare applications, especially when it comes to adopting a wireless healthcare system (i.e., wireless medical sensors, wireless gateways, mobile devices, etc.). Although wireless healthcare offers many advantages to patient monitoring, the physiological data of an individual are highly vulnerable. Further, due to the wireless nature of devices (i.e., medical sensors, iPhone, PDA, etc.), the patients' vital signs are much easier to query and monitor (i.e., in an ad hoc manner) within the hospital ward rooms using smart phones, iPhones, PDAs, and laptops, so any adversary can be eavesdropping on patients locally in the ward room using their hand-devices that could cause of patient privacy breaches. More importantly, the patient vitals are very sensitive; so they (i.e., the patient's vitals) must be kept secure from unauthorized users and security threats. Moreover, government laws (e.g., the Health Insurance Portability and Accountability Act of 1996 (HIPAA)) also regulated stringent rules for healthcare providers, such as; individuals' vital signs are only revealed to authorized professionals (i.e., doctors, caregivers and nurses) and family members. A healthcare provider is subject to strict civil and criminal penalties (i.e., either fine or imprisonment) if HIPAA rules are not followed properly . Furthermore, as wireless medical sensor nodes themselves provide services to users (doctors, nurses, and technicians, are a few examples) it is necessary to control who is accessing their (the medical sensors') information and whether they are authenticated to do so. Therefore, strong user authentication is a core requirement to protect from illegal access to patients' vital signs, and can attain the

highest levels of patients' privacy.

So far many significant researches have been proposed for healthcare using sensor networks and provide sufficient security, such as data confidentiality, authentication, integrity and preserving patient privacy. These schemes do not consider strong user authentication, and hence, lack a security mechanism, according to the HIPAA laws . Further, in the authors proposed a few user authentication protocol for wireless sensor networks, which are either broken or provide less security at very high computation and communication costs. Consequently, to the best of our knowledge, a strong user authentication (i.e., professional authentication) protocol for wireless healthcare applications has not yet been addressed effectively in order to prevent illegal access to wireless medical sensor data.

(1) the healthcare architecture and major security requirements for healthcare application using wireless medical sensor networks;

(2) propose an efficient-strong authentication protocol, named E-SAP, for healthcare applications using WMSNs.

In addition, E-SAP provides secure session key establishment between the users and the medical sensor nodes, and allow users to change their password. Furthermore, we demonstrate the formal verification of the proposed protocol by the Burrows, Abadi and Needham (BAN) logic model , where two main security properties are verified: authenticity and secure session key establishment. Moreover, the proposed scheme resists many practical attacks (e.g., replay, user and gateway masquerade, smartcard stolen-verifier, gateway secret key guessing, password guessing, and information-leakage). To attain the low computational overheads, our scheme uses one-way hash functions along with XOR operations and symmetric cryptosystem.

The rest of paper is organized as follows: Section 2 discusses the healthcare architecture using wireless medical sensors, adversary attack model, and wireless healthcare security requirements. Section 3 briefly reviews the related literature for secure healthcare monitoring using medical sensor networks. Section 4 introduces and describes a novel E-SAP: efficient-strong authentication protocol for healthcare application using WMSNs. Section 5 describes the brief introduction of BAN logic and provides formal verification of E-SAP using the BAN logic model. Section 6 discusses the security analysis and efficiency evaluation in contrast to exiting schemes and finally, in conclusions and future directions are presented.

CLOUD computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application.

A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following Challenging issues. An essential driver of poor site configuration is that the web designers' understanding of how a site ought to be organized can be respectably not quite the same as those of the clients. Such contrasts bring about situations where clients can't without much of a stretch find the coveted data in a site.

This issue is hard to dodge on the grounds that when making a site, web engineers might not have a reasonable understanding of clients' inclination and can just compose pages focused around their own particular judgments. Be that as it may, the measure of site viability ought to be the fulfillment of the clients instead of that of the engineers. Subsequently, Webpages ought to be composed in a manner that by and large matches the client's model of how pages ought to be sorted out. Past studies on site has concentrated on a mixture of issues, for example, comprehension web structures, discovering applicable pages of a given page, mining educational structure of a news site, and concentrating layout from pages.

Our work, then again, is nearly identified with the writing that inspects how to enhance site safety through the utilization of client route information. Different works have attempted to address this inquiry and they can be for the most part characterized into two classifications : to encourage a specific client by rapidly reconstituting pages focused around his profile and traversal ways, regularly alluded as personalization, and to alter the site structure to facilitate the route for all clients, frequently alluded as change. In this paper, we are concerned basically with change approaches. The writing considering changes approaches essentially concentrates on creating routines to totally reorganize the connection structure of a site. In spite of the fact that

there are supporters for site revamping methodologies, their downsides are selfevident. To start with, since a complete rearrangement could profoundly change the area of recognizable things, the new site may perplex clients . Second, the redesigned site structure is very eccentric, and the expense of confusing clients after the progressions stays unanalyzed.

This is on account of a site's structure is commonly composed by masters and bears business or hierarchical rationale, however this rationale might no more exist in the new structure when the site is totally rearranged. Furthermore, no earlier studies have surveyed the ease of use of a totally rearranged site, prompting questions on the pertinence of the revamping methodologies. At long last, since site rearrangement methodologies could drastically change the current structure, they can't be often times performed to enhance the reversibility.

2. LITERATURE SURVEY

2.1 SHAREMIND: A FRAMEWORK FOR FAST PRIVACY-PRESERVING COMPUTATIONS

In this paper et.al(1)D.Bogdanov, S.Laur,J.Willemson (2008) has proposeda provably secure and efficient general-purpose computation system, a 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 the solution is in the choice of the secret sharing scheme and the design of the protocol suite. Many practical decisions have been made 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.

2.2 A PROGRAMMABLE SERVICE ARCHITECTURE FOR MOBILE MEDICAL CARE

In this paper et.al(2) R. Chakravorty (2006) has proposedMobicare - a flexible, programmable architecture that efficiently exploits mobile and wireless communication systems to provide better healthcare services in a wide-range of scenarios. The Mobicare architecture consists of three important building blocks: a Body sensor network (BSN) consisting of wearable sensors and actuators with wireless inter-connections; a BSN Manager (also called Mobicare client) that connects the BSN to an ‘always-on’ wide area communication interface using GPRS or UMTS cellular wireless links; and back-end infrastructure support (Mobicare servers) at healthcare providers to implement necessary healthcare functionalities. A novelty in Mobicare is the remote dynamic software update functionality applied to the native code of the client device. The mechanisms for registration and remote configuration of the body sensors, as well as remote health data services such as health information downloads and diagnosis data uploads with the provider servers have been defined. A prototype for Mobicare as a proof-of-concept is implemented, and evaluated in an experimental wireless test bed consisting of Bluetooth and GPRS/UMTS cellular networks. The evaluation demonstrates Mobicare as a feasible and useful infrastructure paradigm .

2.3PERMUTATION-BASED ENCRYPTION, AUTHENTICATION AND AUTHENTICATED ENCRYPTION

In this work et.al(4) J. Daemen, G.Bertoni, M.Peeters, G.V.Assche (2012) has proposedan alternative based on fixed-width permutations with nodes built on top of the sponge and duplex construction, and concrete proposal Keccak. Permutation based approach is scalable and suitable for high-end CPUs as well as resource-constrained platforms. The latter is illustrated by the small Keccak instances and the sponge functions Quark, Photon and Spongent, all addressing lightweight applications. It is proven that the sponge and duplex construction resist against generic attacks with complexity up to $2c/2$, where c is the capacity. This provides a lower bound on the width of the underlying permutation. However, for keyed nodes and bounded data complexity, a security strength level above $c/2$ can be proven. For MAC computation, encryption and even authenticated encryption with a passive adversary, a security strength level of almost c against generic attacks can be attained. This increase in security allows reducing the capacity leading to a better efficiency. It is argued that for keyed nodes of the sponge and duplex constructions the requirements on the underlying permutation can be relaxed, allowing to significantly reduce its number of rounds. Finally, two generalizations of the spongeis presented and duplex constructions that allow more freedom in tuning the parameters leading to even higher efficiency. It is illustrated that generic constructions with proposals for concrete instantiations calling reduced-round versions of the
Keccak - f [1600] and Keccak - f [200] permutations.

2.4 REAL-TIME AND SECURE WIRELESS HEALTH MONITORING

In this work et.al(5) S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa(2008) has proposeda framework for a wireless health monitoring system using wireless networks such as ZigBee. Vital signals are collected and processed using a 3-tiered architecture.

The first stage is the mobile device carried on the body that runs a number of wired and wireless probes. This device is also designed to perform some basic processing such as the heart rate and fatal failure detection. At
the second stage, further processing is performed by a local server using the raw data transmitted by the mobile device continuously. The raw data is also stored at this server. The processed data as well as the analysis results are then transmitted to the service provider center for diagnostic reviews as well as storage. The main advantages of the proposed framework are
(1) the ability to detect signals wirelessly within a body sensor network (BSN)
(2) low-power and reliable data transmission throughZigBee network nodes
(3) secure transmission of medical data over BSN
(4) efficient channel allocation for medical data transmission over wireless networks
(5) optimized analysis of data using an adaptive architecture that maximizes the utility of processing and computational capacity at each platform.

2.5 PERVASIVE, SECURE ACCESS TO A HIERARCHICAL SENSOR-BASED HEALTHCARE MONITORING ARCHITECTURE IN WIRELESS HETEROGENEOUS NETWORKS

In this work et.al(4) Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park (2009) has proposed a healthcare monitoring architecture coupled with wearable sensor systems and an environmental sensor network for monitoring elderly or chronic patients in their residence. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile computing devices. Three application scenarios are implemented using the proposed network architecture. The group-based data collection and data transmission using the ad hoc mode promote outpatient healthcare services for only one medical staff member assigned to a
set of patients. Adaptive security issues for data transmission are performed based on different wireless capabilities. This study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. The implemented schemes were verified as performing efficiently and rapidly in the proposed network architecture.

METHODOLOGY

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the Untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving access control to users, which guarantees any member in group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

3.1 MODULE DESCRIPTION

The Privacy Protection for wireless medical datahave following modules,

- Group Member Registration and Login
- Batch Level Sign Based Key Generation
- Upload File to Data Cloud Server
- Download File from Data Cloud Server
- Public Auditing with User Revocation in Public Verifier

3.1.1 GROUP MEMBER REGISTRATION AND LOGIN:

The first User enters his username, password, and chooses any one group id then registers with Data Cloud Server. Group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability

3.1.2 BATCH LEVEL SIGN BASED KEY GENERATION:

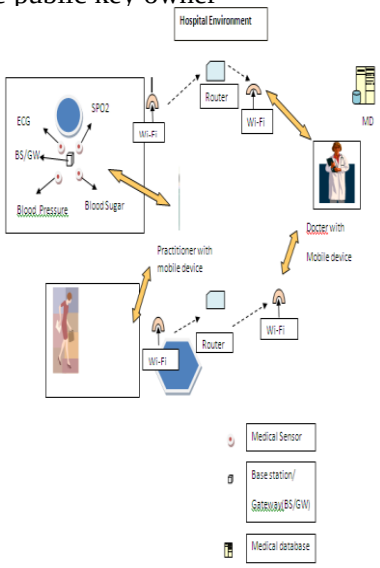
Every user in the group generates his/her public key and private key. User generates a random p, and outputs public key and private key. Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

3.1.3 UPLOAD FILE TO DATA CLOUD SERVER:

The user wants to upload a file. So the user splits the files into many blocks. Next the user encrypts each blocks with his public key.

3.1.4 DOWNLOAD FILE FROM DATA CLOUD SERVER:

The next user or group member wants to download a file. So the user gives the filename and get the secret key. Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient. The intended recipient (or any other party) verifies the signature to determine its authenticity. Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory's public key and identity shall be made available to the verifier in an authenticated manner.The public key may, for example, be obtained in the form of a certificate signed by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner



Patient Monitoring Using A Wireless Medical Sensor Network In A Hospital Environment

3.1.5 PUBLIC AUDITING WITH USER REVOCATION WITH VERIFIER:

The User who entered the wrong secret key will be blocked by the public verifier. Next the user added public verifier revoked user list. User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

4.CONCLUSION:

In order to detect errors in big data sets from sensor net-work systems, a novel approach is developed with cloud computing. Firstly error classification for big data sets is presented. Secondly, the correlation between sensor net-work systems and the scale-free complex networks are introduced. According to each error type and the features from scale-free networks, we have proposed a time-efficient strategy for
detecting and locating errors in big data sets on cloud. With the experiment results from our cloud computing environment U-Cloud, it is demonstrated that

1) the proposed scale-free error detecting approach can significantly reduce the time for fast error detection in numeric big data sets,

2) the proposed approach achieves similar error selection ratio to non-scale-free error detection approaches. In future, in accordance with error detection for big data sets from sensor network systems on cloud, the issues such as error correction, big data cleaning and recovery will be further explored

References

[1] D. Bogdanov, S. Laur, J. Willemson. Sharemind: A Framework For Fast Privacy-Preserving Computations. In Proc. Esorics' 08, Pages 192-206, 2008crypto++ .6.0 Benchmarks. Http://Www.Cryptopp.Com / Benchmarks.Html.

[2] R. Chakravorty. A Programmable Service Architecture For Mobile Medical Care. In Proc. 4th Annual Ieee International Conference On Pervasive Computing And Communication Workshop (Persomw'06), Pisa, Italy, 13-17 March 2006..

[3] J. Daemen, G. Bertoni, M. Peeters, G. V. Assche, Permutation-Based Encryption, Authentication And Authenticated Encryption, Diac'12, Stockholm, 6 July 2012..

[4] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Real-Time And Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, Doi: 10.1155/2008/135808.

[5] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access To A Hierarchical Sensor-Based Healthcare Monitoring Architecture In Wireless Heterogeneous