ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Privacy Protection for Wireless Medical Sensor Data

D.Thiyagarajan[1], M.Logambika[2], S.Nandhini[3], K.Manikandan[4]
Assistant Professor[1], Final year students[2,3,4] , Department of Computer Science and Engineering
K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India
logambika611@gmail.com, nandhinismart55@gmail.com, manikarnan95@gmail.com

Abstract: 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.

Keywords:

Wireless medical sensor network, patient data privacy, Paillier encryption, and ElGamal encryption.

1. Introduction

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. Storing data in the cloud has become a trend. An increasing number of clients store their important data in remote servers in the cloud, without leaving a copy in their local computers. Sometimes the data stored in the cloud is so important that the clients must ensure it is not lost or corrupted. While it is easy to check data integrity after completely downloading the data to be checked, downloading large amounts of data just for checking data integrity is a waste of communication bandwidth. Hence, a lot of works have been done on designing remote data integrity checking protocols, which allow data integrity to be checked without completely downloading the data. Remote data integrity checking is first introduced in which independently propose RSA-based methods for solving this difficult problem use this checking protocols: data dynamic, public verifiability and privacy against verifiers. The system in support data dynamics at the block level, including block insertion, blocks modification and block deletion. It supports data append operation. In addition, can be easily adapted to support data dynamics can be adapted to support data dynamics by using the techniques. On the other hand, It support public verifiability, by which anyone (not just the client) can perform the integrity checking operation. The system in support privacy against third party verifiers. Compare the proposed system with selected previous system.

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. Some security and privacy issues that need to be considered are as follows 1) Authentication: Only authorized user can access data in the cloud. 2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure. 3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data. 4) No storage Overhead and easy maintenance: User doesn't have to worry about the storage requirement & maintenance of the data on a cloud. 5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user. 6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation. In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done.

2. Literature Survey

In [1] authors developed a method 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. Atthe 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.

In [2] authors presents 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.

In [3] authors described ALARM-NET, a wireless sensor network for assisted-living and residential monitoring. It integrates environmental and physiological sensors in a scalable, heterogeneous architecture. A query protocol allows real-time collection and processing of sensor data by user interfaces andback-end analysis programs. One such program determines circadian activity rhythms of residents, feeding activity information back into the sensor network to aid context-awarepower management, dynamic privacy policies, and data association. Communication is secured end-to-end to protect sensitive medical and operational information. The ALARM-NET system has been implemented as a network of

MICAz sensors, stargate gateways, iPAQ PDAs, and PCs. Customized infrared motion and dust sensors, and integrated temperature, light, pulse, and blood oxygenationsensors are present.

In [4] author presents the eHealth system is envisioned as a promising approach to improving health care through information technology, where security and privacy are crucial for its success and large scale deployment. In this paper, we propose a strong privacy preserving Scheme against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve not only thecontent oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the effectiveness and practicability of the proposed scheme.

In [5] author proposed a two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptograph problems of long standing.

In [6] author develop this Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

3. Proposed Work

The proposed work is mainly focused on 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.

Group Member Registration and Login

The first User entered his username, password, and chooses any one group id then register 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.

Batch Level Sign Based Key Generation

In 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.

Algorithms are contains these steps:

Paillier Public key Cryptosystem:-

1) Public key Cryptosystem is the use of asymmetric algorithms, where the key used to encrypt the message is not same as the key used encrypt it.

2) Each user pair of cryptographic keys- a public key & a private key.

3) The private key is kept secret, whilst the public key may be widely distributed.

4) Messages are encrypted with the recipient public key and can only be decrypted with the corresponding private key.

ElGamal Public key Cryptosystem:-

1)Different keys are used for encryption and decryption.

2)Each receiver possesses a unique decryption key, generally referred to as his private key.

3) Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the cipher text and the encryption (public key).

4)This signature algorithm is similar to the encryption algorithm in that the public key and private key.

Upload files to Cloud server

The user wants to upload a file. So he split the files into many blocks. Next he encrypt each blocks with his public key using algorithm.

Download file from cloud server

The next user or group member wants to download a file. So he 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 (Certification Authority) or in a face-to-face meeting with the public key owner.

Public Auditing with user revocation in public verifier

The User who entered the wrong secret key then he blocked by the public verifier. Next he 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.

Reference

[1] 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.

[2] 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 Networks. IEEE J.

Select. Areas Commun. 27: 400-411, 2009.

[3] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S.Lin, J.Stankovic. Alarm-Net: Wireless Sensor Networks For Assisted-Living And Residential Monitoring. Technical Report Cs-2006-01; Department Of Computer science, University Of Virginia: Charlottesville, Va, USA, 2006.

[4] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato. Sage: A Strong Privacy-Preserving Scheme Against Global Eavesdropping For Ehealth System. IEEE J. Select. Area Commun. 27: 365-378, 2009.

[5] W.Diffie and M. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22 (6): 644-654, 1976.

[6] Digital Signature Standard (DSS). Fips Pub 186-4, July 2013.