International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 98-102 www.ijaem.net ISSN: 2395-5252

Electronic Health Record Maintenance System Using Blockchain Technology

Poorani L[1], Geetha B G[2]
Student, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu[1]
Assistant Professor, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu[2]

Submitted: 01-05-2021 Revised: 09-05-2021 Accepted: 10-05-2021

ABSTRACT: 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.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 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.

I. INTRODUCTION

1.1 privacy preserving cloud computing

During the last few years, we have seen the 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.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.A typical patient monitoring in hospital environment.Several research groups and projects are working in health monitoring using wireless sensor networks, for example, CodeBlue [2], LiveNet [3], MobiHealth [4], UbiMon [5], Alarm-Net [6], ReMoteCare [7], SPINE [8], etc. Thus, healthcare systems are the applications that most benefit from using wireless medical sensor technology that can perform patient care within hospitals, clinics and homecare.

1.2 privacy-preserving public auditing for data storagesecurity in cloud computing

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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 98-102 www.ijaem.net ISSN: 2395-5252

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 problem. After that propose a remote storage auditing method based on pre-computed challenge-response pairs.

Recently many works focus on providing three advanced features for remote data integrity 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.

1.3 Dynamic Provable Data Possession In Medical Data Management:

As storage-outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention. In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data).

However, the original PDP scheme applies only to static (or append-only) files. Present a definitional framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. Use a new version of authenticated dictionaries based on rank information. The price of dynamic updates is a performance change from O(1) to O(log n) (or O(nlogn)), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g., 415KB proof size and 30ms computational overhead for a 1GB file). Show how to apply our DPDP scheme to outsourced file systems and version control systems (e.g., CVS).

II. MODULE

2.1 Group Member Registration And Login

In this module 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

2.2 Batch Level Sign Based Key Generation

In Key Generation module, 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.

2.3 Upload Files To Cloud Server

In this module the user wants to upload a file. So he split the files into many blocks. Next he encrypt each blocks with his public key.

2.4 Download File From Cloud Server

In this module 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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 98-102 www.ijaem.net ISSN: 2395-5252

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.

2.5 Public Auditing With User Revocation In Public Verifier

In this module, 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.

III. EXISTING SYSTEM

In existing system 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. In the existing System data owners store the encrypted data files in un trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as wells storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the data owners and the number of revoked users, respectively.In existing system for providing privacy to the medical sensor networks is a medical care application used or home patient monitoring and it is more secured than the other key based solution which ensure security for the sensitive data during transmission. The other existing solutions can provide security against outside attacks but this system assures security for both outside as well as inside attacks where the inside attacker is the administrator of the patient database. This approach utilizes an effective system known as In existing system which is capable of processing the encrypted data without converting it to the decrypted format. In existing system comprises of three servers used for processing patient data and storing in their respective back end databases. They have a unique capability of splitting the patient's health attribute value into three random parts and send them to three servers. The secret keys are pre-deployed in bio sensors and data servers to provide a secure channel for transmission. The data servers can perform computations on the data when the doctors or medical researchers issue commands requesting to access patient data. The main limitation of this system is that it is limited to only 3 servers and is not flexible to add more number of servers for better security.

IV. PROPOSED SYSTEM DESCRIPTION

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.

V. RESULTS AND DISCUSSION

Comparing results when data are on disk versus in cache shows that disk throughput bounds IB-DPDP's performance when accessing all blocks. With the exception of the first blocks of a file, I/O and the challenge computation occur in parallel. Thus, IB-DPDP generates proofs faster than the disk can deliver data: 1.0 second versus 1.8 seconds for a 64 MB file. Because I/O bounds performance, no protocol can outperform IB-DPDP by more than the startup costs. While faster, multiple-disk storage may remove the I/O bound today. Over time increases in processor speeds will exceed those of disk bandwidth and the I/O bound will hold. Sampling breaks the linear scaling relationship between time to generate a proof of data possession and the size of the file. At 99% confidence, IB-DPDP can build a proof of possession for any file, up to 64 MB in size in about 0.4 seconds. Disk I/O incurs about 0.04 seconds of additional runtime for larger file sizes over the in-memory results. Sampling performance characterizes the benefits of IB-DPDP. Probabilistic guarantees make it practical to use public-key cryptography constructs to verify possession of very large data sets. Table 1 and 2 shows the preprocessing accuracy and overall accuracy of the proposed and existing system.

VI. 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.

ACKNOWLEDGEMENT

This work is supported by the staffs in Department of Computer Science and Engineering in K.S.Rangasamy College of Technology (2020-2021).

REFERENCE

[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 Journal 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 Eterogeneous Networks. Ieee J. Select. Areas Commun. 27: 400-411, 2009.

[6]. D. Malan, T. F. Jones, M. Welsh, S. Moulton. Codeblue: An Ad-Hoc Sensor Network Infrastructure For Emergency Medical Care. In Proc. Mobisys 2004 Workshop On Applications Of Mobile Embedded Systems (Wames'04), Boston, Ma, Usa, 6-9 June 2004.

[7]. J. Misic, V. Misic. Enforcing Patient Privacy In Healthcare Wsns Through Key Distribution Algorithms. Secur.Commun. Network 1: 417-429, 2008.

[8]. 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 Computerscience, University Of Virginia: Charlottesville, Va, Usa, 2006.

[9]. F. Hu, M. Jiang, M. Wagner, D. C. Dong. Privacy-Preserving Telecardiology Sensor Networks: Toward A Low-Cost Portable Wireless Hardware/Software Codesign. Ieee Trans. Inform. Tech. Biomed, 11: 619-627, 2007.

[10]. X. H. Le, M. Khalid, R. Sankar, S. Lee. An Efficient Mutual Authentication And Access Control Scheme For Wireless Sensor Network In Healthcare. J. Networks 27: 355-364, 2011.

[11]. 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.

[12]. S. Raazi, H. Lee, S. Lee, Y. K. Lee. Bari+: A Biometric Based Distributed Key Management Approach For Wireless Body Area Networks. Sensors 10: 3911-3933, 2010.

[13]. W. Diffie And M. Hellman. New Directions In Cryptography. Ieee Transactions On Information Theory, 22 (6): 644-654, 1976.

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

[15]. P. Kumar And H. J. Lee. Security Issues In Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012.

[16]. H. J. Lee And K. Chen. A New Stream Cipher For Ubiquitous Application. In Proc. Iccit'07, South Korea, 2007.

[17]. K. Malasri, L. Wang. Design And Implementation Of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009.
[18]. R. Rivest, A. Shamir, And L. Adleman. A Method For Obtaining Digital Signatures And Public-Key Cryptosystems. Communications Of The Acm, 21 (2): 120-126, 1978.
[19]. A. B. Waluyo, I. Pek, X. Chen, W.-S.Yeoh. Design And Evaluation Of Lightweight Middleware For Personal Wireless Body Area Network. Pers. Ubiquit. Comput, 13: 509-525, 2009.
[20]. Sha-3 Standard: Permutation-Based Hash And Extendable- Output Functions. Draft Fips Pub 202, May 2014.
[21]. Azzedineboukerche, And Yonglinren," A Secure Mobile Healthcare System Using Trust-Based Multicast Scheme",Ieee Journal On Selected Areas In Communications, Vol. 27, No. 4, May 2009,316-325.
[22]. Daojing He, Sammy Chan, Member, Ieee, And Shaohua Tang, Member, Ieee," A Novel And Lightweight System To Secure Wireless Medical Sensor Networks", Ieee Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014,23-32
[23]. Rongxing Lu, Member, Ieee, Xiaodong Lin, Member, Ieee, And Xuemin (Sherman) Shen, Fellow, Ieee," Spoc: A Secure And Privacy-Preserving Opportunistic Computing Framework For Mobilehealthcare Emergency", Ieee Transactions On Parallel And Distributed Systems, Vol. 12, No. 2, May 2012,452-461.
[24]. Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, And Hua Fang," Ecg- Cryptography And Authentication In Body Area Networks", Ieee Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November 2012,321-332.
[25]. 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.