ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.02, Issue.11
November -2020
Pages: -219-224

SECURE ORGANIZATIONAL DATA SHARING BETWEEN USERS USING DIFFIE-HELLMAN

[1] REDDEM VASUDEVA REDDY, [2]Guide, KAMBHAM SALIVAHANA REDDY, M. tech (Assistant professor)

[1,2]Global College of Engineering and Technology, Department CSE

ABSTRACT:

Cloud computing is an emerging technology which provides various types of facilities to the users. Cloud computing is based on the concept of storage, virtualization, and connectivity and processing power to store resources and these resources are shared between different computers and other devices via the internet. To ensure the security of cloud computing is the challenging issue in the cloud environments. By using cloud computing, it becomes easier to access and use personal information in the Cloud. In order to provide the security to the cloud network, homomorphic encryption technique is applied at the virtual machine for the verification and encryption/decryption of the user. But due to the lack of key sharing and key management feature, we apply Diffie-Hellman algorithm at the virtual machine for the authentication of the user. Diffie Hellman algorithm allows two parties to communicate with each other and also exchange their secret keys over an unprotected communication channel without meeting in advance.

Keywords: Cloud Computing, Diffie Hellman Algorithm Decryption, Encryption, Homomorphic Encryption Scheme, Security

INTRODUCTION: Cloud computing is a new promising technology that leverages the user from the burden of hardware maintenance and offers dynamically flexible and scalable computational resources accessible from any place where a network is available. The emergence of this paradigm has deeply influenced many domains and especially the healthcare sector. However, the usage of this model in the healthcare domain needs the reinforcement of security measures because data are susceptible to lose, leakage or theft. Therefore, confidentiality and integrity of the stored Electronic Health Records (EHR) are deemed as one of the major challenges elevated by the external storage. Besides, the privacy of sensitive data must be guaranteed. To overcome the above cited challenges, cryptographic techniques for securing e-health systems are widely adopted. But the reliance on a single cloud storage provider has shown many drawbacks like a single point of failure, vendor lock-in and malicious insiders. To narrow down the listed disadvantages, it is advisable to use multi-cloud architecture. One of the key concepts of this model is to store data on different cloud server providers where an insider is not able to reconstruct the original data from a single share [1]. In this context, several solutions have been proposed in the literature to ensure secure multi-cloud storage in e-health systems [2–5]. They mainly have two phases: *storage* and *retrieval*. They also all use cryptographic primitives to ensure EHRs security. Authors of [2] use an Attribute Based-Encryption (ABE) for selective access authorisation and cryptographic secret sharing. The EHRs split and reconstruction is done through a proxy. In [3], ABE is used for selective data sharing with physicians without allowing them to know the precise description of the patient's illnesses. Biometrics based authentication and Kerberos tickets session are used in [4] to guarantee secure interaction with the EHR system. In addition, a steganographic technique is used to store EHR. In [5], authors propose the use of Shamir's Secret Sharing not only to distribute EHR

Copyright @ 2020 **ijearst. All rights reserved.**

shares among cloud servers but to retrieve the requested EHR from partial cloud servers. In summary, the main drawback of [2–5] is the reliance on a trusted third party which may not be adequate for practical use as they show security risks. Hence, a secure privacy-preserving data storage solution is still needed to improve the patient role to monitor his data on the cloud.

In this paper, we present a Hybrid and Secure Data Sharing Architecture (HSDSA), for secure and privacy-preserving storing and sharing of patient's sensitive data in a Multi-cloud environment without relying on a trusted third party. In HSDSA, cloud providers are assumed to be semi-trusted: honest but curious. HSDSA gives the patient total control over the generation and management of the decryption keys without relying on a trusted authority and thus it is more applicable for public cloud environments. To protect the data from external attackers, Rivest–Shamir–Adleman (RSA) encryption is applied before outsourcing EHR. To secure data against cloud providers curiosity, Shamir's secret sharing is adopted. The resulted shares are distributed to multiple clouds. To download an EHR, HSDSA recovers its shares using an outsourcing reconstruction operation based on the (t, n) strategy. To complete the file decryption, a Schnorr-based technique is used to prove data possession and to verify the requester identity. Then a session, using the Diffie Hellman (DH) algorithm, is created to securely exchange the decryption key. Finally, the key is extracted and the original EHR could be recovered. Outsourcing reconstruction operation based on the (t, n) strategy is used.

2. LITERATURE REVIEW

Cloud deployment models: In cloud computing, there are different models used for cloud storage that allow users to maintain control over their data. These deployment models are: private, public or hybrid. A private cloud means using their own resources and own data centers making organization in control. The resources used in private cloud are not shared with other customers. "The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party. Resources are dedicated only to the customer." While in public cloud, organization will be relieved from the management but the organization have less control. Architectural layers of Cloud Computing: a) Software as a service (SaaS): This features a complete application offered as a service on demand. b) Platform as a service (PaaS):The goal of this layer is to enable the developers to build their own applications.c) Infrastructure as a service (IaaS): Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Security issues in Cloud Computing: According to NIST's definition, information security is the practice of maintaining the integrity, confidentiality and availability of data from malicious access, system failure and etc. **Integrity:** It means the information provided is authentic, complete and trustworthy. The data over the cloud shall not be changed or altered by any unauthorized user or by any malicious activities.

Confidentiality: Confidentiality means information is accessed only by an authorized person or shared among authorized groups. An authentication method includes credential verification that can be applied to protect data against malicious attack.

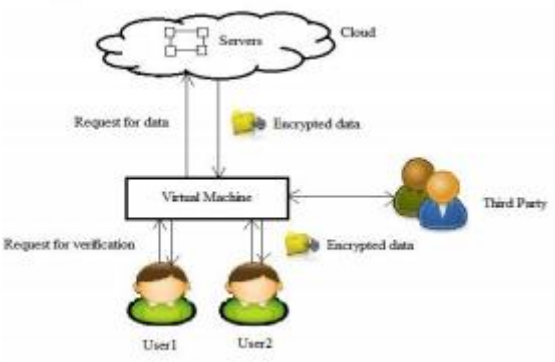
Availability: It refers to the availability of the requested data resource. Data should be available under authorized operation including read, write and etc. Since cloud computing is utility available on internet, so various issues like user privacy, data theft and leakage and unauthenticated accesses are raised. To solve this problem concept of cryptography issued. Cryptography is the science of securely transmitting and retrieving information using an insecure channel. Cryptography involves two processes: encryption and decryption. Encryption is a process in which sender converts data in form of an un recognized string or cipher text for transmission, so that an eavesdropper could not know about the data. Decryption is just the reverse of encryption. The receiver transforms sender's cipher text into a meaningful text known as plaintext. Homomorphic Encryption Homomorphic Encryption systems are used to perform various operations on the encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. For Example: RSA Cryptosystem In general,

Copyright @ 2020 **ijearst. All rights reserved.**

if n number of persons wants to communicate then they requires n * (n-1) / 2 number of keys. To solve this problem, the Diffie-Hellman key exchange protocol is used. This protocol provides a one-time session key for two parties. Diffie-Hellman Algorithm One of the major issue of public-key encryption is to address the problem of key distribution.

3. Implementation:

The motivation for running the Diffie-Hellman protocol is to implement a secure session over an insecure network connection.



1. In the first step, the users send the request to the virtual machine for verification. 2. After verification, if the user is authorized then the virtual machine send the request to the cloud server for the data. 3. The data is send to the virtual machine in the encrypted form to protect it from an un- authorized user. 4. Then the secure path is established between the user and the virtual machine and the data is send to the user. 5. At user's end, the data is decrypted by using user's private key. 6. To create a secure communication path Diffie-Hellman algorithm is used at the virtual machine. 7. For encryption and decryption of data, basic homomorphic encryption scheme is used. 8. If the user is not authorized then no connection is made between user and virtual machine

Our research focus on various threats that are the major issue for anyone when they want to adopt the cloud services for their work. To resolve this problem, a framework should be designed for the execution of data and information securely in the cloud environment. It will protect users' data, messages, information from an unauthorized access.

Methodology:

This study is mainly focused on to develop a model for fully homomorphic disk encryption schemes. The new scheme will provide reliable key storage and key management services. In this new model, secure channel establishment algorithm i.e. Diffie-Hellman algorithm will used for key management and key sharing. The Diffie- Hellman algorithm is most secure and reliable algorithm. We have embedded the Diffie Hellman key exchange algorithm for authentication procedure. In cloud network, it defines the source node and destination node. To establish secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties. The source node become master and destination node become slave, master and slave select their private keys 'a', 'b' respectively. The master calculates new value "M" from their selected public and private numbers. 1. M= ga mod n The Slave calculates new value "S" from their selected public and private numbers 2. S= gb mod n The Master and slave exchange their calculated "M" and "S" values through intermediate nodes. 3. When Slave receives "M" and Master receives "S" both parties will calculate mode inverse value. When master receive value "S" from slave and calculate new value "K1" from the received "S" value. 4. K1=Sa mod n Slave receives value "M" from master and calculates new value"K2" from the received "M" 5. K2=Mb mod n After calculating "K1" and "K2", both parties

Copyright @ 2020 **ijearst. All rights reserved.**

establish secure channel, by calculated new key "K". If both communicating parties have same "K1" and "K2" values, secure channel is established between Master and Slave. K=K1+K2 When secure channel is established between master and slave, communication starts between both parties. The communication between Master and Slave is encrypted with public keys. Each parties use their own private keys to decrypt the communication. In our work, we are using Diffie-Hellman algorithm for secure channel establishment and for mutual authentication. In our proposed scheme only two messages are needed to exchange between two devices and a secure channel will be established. It is more secure than the existing authentication procedure. It takes less time to authenticate the users and it enhances the performance of the mobile devices in the network.

4. Conclusion:

The numerous benefits provided by the cloud have driven many large multilevel organizations to store and share their data on it. This paper begins by pointing out major security concerns data owners have when sharing their data on the cloud. Next, the most widely implemented and researched data sharing schemes are briefly discussed revealing points of weakness in each. To address the concerns, here propose a Secure Organizational data sharing between users using Diffie-Hellman scheme that allows data to be shared efficiently and securely on the cloud. Hellman scheme partitions a data file into multiple segments based on user privileges and data sensitivity. Each segment of the data file is then shared depending on data user privileges. We formally prove that Hellman scheme is secure against adaptively chosen plaintext attack assuming that the DBDH assumption holds. Our comprehensive performance and simulation comparisons with the three most representative schemes show that Hellman scheme can significantly reduce the computational complexity while minimizing the storage space. Our proposed scheme lays a foundation for future attribute-based, secure data management and smart contract development

REFERENCES [1] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 200 9. [2] Yogesh Kumar, Rajiv Munjal andn Harsh Sharma Comparison of Symmetric and Asymmetric Cryptography With Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and anagement Studies, Vol. 11, Issue 03, Oct 2011. [3] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009. [4] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3- DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013. [5] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010). [6] Mr. Mukta Sharma and Mr. Moradabad R. "Comparative Analysis of Block Key Encryption Algorithms "International Journal of Computer Applications (0975 – 8887) Volume 145 – No.7, July 2016. [7] AshimaPansotra and SimarPreet Singh "Cloud Security Algorithms" International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360. [8] Iram Ahmad and Archana Khandekar "Homomorphic Encryption Method Applied to Cloud Computing" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530. [9] Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures by Yogesh Kumar, Rajiv Munjal, and Harsh ,(IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853. [10] Comparative analysis of performance efficiency andsecurity measures of some encryption algorithms y AL,Jeeva, Dr.V.Palanisamy, K.Kanagaram compares symmetric and asymmetric cryptography algorithms ISSN: 2248-9622. [11] New Comparative Study Between DES, 3DES and AES within Nine Factors Hamdan.O.Alanazi, B.B.Zaidan, . A.Zaidan, Hamid A,Jalab, M.Shabbir and Y. Al- Nabhani JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH

Copyright @ 2020 **ijearst. All rights reserved.**

2010,ISSN 2151-9617. [12] Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi, SanjayAgrawal compares Symmetric and AsymmetricCryptographyTechniques using throughput, key length, tunability, speed, encryption ratio and security attacks. IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 ISSN (Online): 2231-5268 [13] Evaluation of Blowfish Algorithm based on Avalanche Effect by Manisha Mahindrakar gives a new performance measuring metricavalanche effect. International Journal of Innovations in Engineering and Technology (IJIET) 2014. [14] Mr. Gurjeevan Singh, Mr.Ashwani Singla And Mr. K S Sandha "Cryptography Algorithm Compassion for Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011. [15] Mr.Milind Mathur and Mr. Ayush Kesarwani "Comparison between DES, 3DES, RC2, RC6, Blowfish and AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013. [16] urpreet Singh, SupriyaKinger "Integrating AES, DES, and 3-DES Encryption Algorithm for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013. [17] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 First International Conference On parallel, Distributed and Grid Computing (PDGC-2010). [18] AnnapoornaShetty , ShravyaShetty K , Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014 [19] RFC2828],"Internet Security http://www.faqs.org/ rfcs/rfc2828.html. [20] Aamer Nadeem et al, "A rformance Comparison of Data Encryption Algorithms", IEEE 2005.

Copyright @ 2020 **ijearst. All rights reserved.**