International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Multi-Level Cryptographic Key Sharing For Secure Access and Authorization on Cloud Platforms - A Review

Kuldeep Singh[1], Er. Amardeep Kaur[2]

[1, 2]Desh Bhagat University, Mandi Gobindgarh,

Abstract: ***Cloud computing is attracting the large user bases and now-a-days hosting the large sized application with heavy and complex calculation load. The cloud computing platforms are because being popular and user at large scales, they are also being favorite targets of the hacking groups. Some cloud computing application carry secure and personal data, which may affect the social image, security or economics of a nation, personnel, organization or other similar entities. Hence, there is always a strong requirement of the secure authorization & request and data exchange model. The security is continuous process, and the models are kept changing from time to time. Effective & Secure key management and distribution scheme play an important role for the data security in Cloud Computing. The cryptographic keys are used on different communication levels of Cloud Computing communications i.e. neighbor nodes, cluster heads and base stations. We proposed a new model presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. In this research, we will develop the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. To add more security, there is a next step which includes Captcha, user has to fill the correct given Captcha which eliminates the possibility of robot, botnet etc. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud computing platforms.***

Keywords: Cloud Storage, Data Security, Data Encryption, Cryptographic keys, Security Attacks, Cloud Computing

1. Introduction

Cloud computing enables on-demand access to computing and data storage resources that can be configured to meet unique constraints of the clients with minimal management overhead. The recent rise in the availability of cloud services makes them attractive and economically sensible for clients with limited computing or storage resources who are unwilling or unable to procure and maintain their own computing infrastructure. The ever increasing need for computing power and storage accounts for the steady growth in popularity of companies offering cloud services. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud. The main drawback, however, is security and in particular data confidentiality: Users of cloud technology essentially have to trust that the cloud providers do not misuse their data. The recent disclosure of the PRISM surveillance program3 in which NSA directly monitors all communication going through most world-wide cloud providers such as Yahoo, Google, and Microsoft, is just one out of several incidents emphasizing that this concern about security is real.

To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email data, and personal preferences are stored on web portal sites such as Google and Yahoo. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services.

One method for alleviating some of these problems is to store data in encrypted form. We are proposing a new model presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. In this research, we will develop the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. We are adding one more level of security in which user has to match the given captcha to access the data, when user matches the captcha, he/she will be able to view or access the data. It eliminates the possibility of botnet, spam or robot etc.

2. Literature Review

A literature review is all about the study of the literature, information of existing techniques and our field of research . While the form of the literature review may vary with different types of studies, but the basic purposes remains same. The main literature surveys are given as:

(1) Zongwei Zhou et. al. proposed "a Key management algorithm named as Key it Simple and Secure (KISS). This paper presents a new key management architecture, called KISS, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. KISS protects the entire life cycle of cryptographic keys. In particular, KISS allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to KISS and verify system output.

(2) N. Suganthi, V. Sumathy, "This algorithm supports the establishment of three types of keys for each sensor node, an individual key shared with the base station, a pair wise key shared with neighbor sensor node, and a group key that is shared by all the nodes in the network. The algorithm used for establishing and updating these keys are energy efficient and minimizes the involvement of the base station. Polynomial function is used in the study"

(3) Ivan Damgård et. al. proposed "A secure key management method for cloud environments. Authors have studied the levels of security on the basis what they can and what they cannot obtain in the security models. And after studying that all, authors have proposed a light-weight protocols achieving maximal security, and report on their practical performance. They have considered fully autonomous servers that switch between online and offline periods without communicating with anyone from outside the cloud, and semi-autonomous servers that need a limited kind of assistance from outside the cloud when doing the transition. "

(4)Ramaswamy Chandramouli et. al. have worked on " **Cryptographic Key Management Issues & Challenges in Cloud Services.** An analysis of the common state of practice of the cryptographic operations that provide those security capabilities reveals that the management of cryptographic keys takes on an additional complexity in cloud environments compared to enterprise IT environments due to: (a) difference in ownership (between cloud Consumers and cloud Providers) and (b) control of infrastructures on which both the Key Management System (KMS) and protected resources are located. This document identifies the cryptographic key management challenges in the context of architectural solutions that are commonly deployed to perform those cryptographic operations."

(5)Marco Tiloca et. Al. proposed, "Wireless Sensor Networks (WSNs) are currently used in many application scenarios, including industrial applications and factory automation. In such scenarios, Time Division Multiple Access (TDMA) is typically used for data communication among sensor nodes. However, TDMA-based WSNs are particularly prone to Selective Jamming attack, a specific form of Denial of Service attack aimed at severely thwarting network reliability. In this paper, we present SAD-SJ, a self-adaptive and decentralized MAC-layer solution against selective jamming in TDMA-based WSNs. SAD-SJ does not need a central entity, requires sensor nodes to rely only on local information, and allows them to join and leave the network without hindering other nodes activity. We show that SAD-SJ introduces a limited overhead, in terms of computation, communication and energy consumption."

(6)Md. Monzur Morshed et. Al. proposed, "Cluster Based Secure Routing Protocol (CBSRP) is a MANET routing protocol that ensures secure key management and communication between mobile nodes. It uses Digital Signature and One Way Hashing technique for secure communication. According to CBSRP, it forms a group of small clusters consist of 4-5 nodes and after that the communication takes place between mobile nodes. Inside a cluster, there is always a cluster node or cluster head. The cluster head inside the cluster is not permanent as other nodes stay in the queue and based on the priority new cluster node or cluster head is elected from rest of the node. Inside a cluster, mobile nodes are authenticated using One Way Hashing concept and Digital Signature is not necessary inside cluster communication. For Cluster-Cluster authentication we proposed to use Digital Signature. CBSRP ensures secure communication which will be energy efficient as we segmented the whole network into small set of clusters."

3. Methodology

First step towards the research is the literature study of the existing algorithms for key sharing and authentication schemes for the cloud platforms. Literature study will lead towards the development of the new key exchange scheme to ensure the legitimate user session and data communication security. This is also very important to get the architecture of the existing key exchange and authentication schemes for clouds in order to know their merits and demerits. This project would be implemented in the **MATLAB** Simulator. A thorough performance and feature testing model would be formed and utilized to analyze the performance of the cloud security model based upon the key exchange scheme, to detect the flaws and to recover them.

4. Problem Formulation

Cloud computing is attracting the large user bases and now-a-days hosting the large sized application with heavy and complex calculation load. The cloud platforms are economically competent, rather winners than the existing IT infrastructure and also comes pre-embedded with the high level features. The cloud computing platforms are because being popular and user at large scales, they are also being favorite targets of the hacking groups. Some cloud computing application carry secure and personal data, which may affect the social image, security or economics of a nation, personnel, organization or other similar entities. Hence, there is always a strong requirement of the secure authorization & request and data exchange model. The security is continuous process, and the models are kept changing from time to time. In the existing model, the key exchange model is applicable to ensure the security of the cloud platforms. The existing model uses a set of keys stored locally between the cloud servers in the cluster. A server needs to rebuild the encryption key after waking up from the sleeping period. The existing model utilizes the Diffie-Hellman key agreement scheme, which is not up to the mark and have become older scheme. Now-a-days this scheme is not considered secure against the Man in the Middle attack.

Diffie-Hellman is also prone to various kinds of service denial and information stealing attacks. Because of all these reasons, the existing scheme must be improved in order to make it stronger against the attacks, which are possible on the existing scheme. In the proposed model, we are trying to solve the key-problem of data integrity and confidentiality using the effective random key exchange scheme with secure user authorization model.

5. Proposed Model

None of the current commercial systems (either based on software or hardware security modules) or research proposals adequately address both challenges with small and simple Trusted Computing Base (TCB) for the Cloud Computing platforms. The proposed model in this research presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Multi-Level CK-EAM protects the entire life cycle of cryptographic keys in the Cloud Computing platforms and applications. In particular, Multi-Level CK-EAM allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to Multi-Level CK-EAM and verify system output. In this research, we will develop the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. To add more security, there is a next step which includes Captcha, user has to fill the correct given Captcha which eliminates the possibility of robot, botnet etc. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud Computing platforms.

6. Conclusion and Future Work

The proposed model for Multi level cryptographic key for secure access has been implemented using the MATLAB simulator. The implementation of the MATLAB simulator will begin with the implementation of the Multi level cryptographic key for secure access. In future, this research presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Multi-Level CK-EAM protects the entire life cycle of cryptographic keys in the Cloud Computing platforms and applications. In particular, Multi-Level CK-EAM allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to Multi-Level CK-EAM and verify system output. In future, the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud Computing platforms. The proposed model will be enhanced for the higher level of security and data privacy using different cryptographic keys.

References

[1] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate KeyManagement", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.

[2] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[3] Ivan Damgård, Thomas P. Jakobsen, JesperBuus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[4] RamaswamyChandramouli, Michaela Iorga, SantoshChokhani, " **Cryptographic Key Management Issues & Challenges in Cloud Services",** Computer Security Division Information Technology Laboratory, NIST, 2013.

[5] Marco Tiloca, Domenico De Guglielmo, GianlucaDini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE, 2013.

[6] Md. MonzurMorshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE, 2013.

[7] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".

[8] SonamPaldenBarfungaPrativaRai, Hiren Kumar Deva Sarma, "Energy Efficient Cluster Based Routing Protocol for Wireless Sensor Networks", ICCCE IEEE 2012, 3-5 July 2012, Kuala Lumpur, Malaysia

[9] SajalSarkar, Raja Datta, "A Trust Based Protocol for Energy-Efficient Routing in Self-Organized MANETs", IEEE 2012.

[10] Said BEN ALL*, Abdellah EZZATI, Abderrahim BENI HSSANE, MoulayLahcen HASNAOUI, "Hierarchical Adaptive Balanced energy efficient Routing Protocol (HABRP) for heterogeneous wireless sensor networks", IEEE, 2010

[11] XU Jiu-qiang, WANG Hong-chuan,LANGFeng-gao,WANGPing,HOU Zhen-peng, "Study on WSN Topology Division and Lifetime", IEEE, 2011