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

Multi-Level Complex Key Sharing For Secure Access and Authorization on Cloud Platforms

Jaskarandeep Punia[1], Rajesh Kumar Bawa[2]

[1]M. Tech Research Scholar, Punjabi University, Department of Computer Science, Patiala, Punjab, India

[2]Professor, Punjabi University, Department of Computer Science, Patiala, Punjab, India

Abstract: ***Cloud computing is an emerging technology used for the large, small or medium enterprise applications, which usually exchange and stores larger amount of data. The cloud computing platforms provide space to a number of applications every year, which also increases the overall user base of the cloud computing infrastructures. The cloud computing application are now also being popular in the users with the touch based portable devices like smart phones, tablet PCs, etc. The cryptographic keys are used on different communication levels of Cloud inter-node communications i.e. clients, servers and other cloud nodes. An effective corporate key management and distribution policy is required to maintain the security of the cloud environments. This research project will be based on secure key management architecture for cloud environments to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Secure Key Exchange will protect the entire life cycle of cryptographic keys in the cloud environment. In particular, Secure Key Exchange will allow only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to Secure Key Exchange and verify system output. In this research project, we will make the Simple and Secure corporate key management technique adaptable for almost all cloud environments.***

Keywords: cloud computing, cloud security, key management, secure authorization and access, multilevel keys.

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. Now a day the availability of cloud services is rising which is making them attractive and economically sensible for clients having limited storage or computing resources who are not willing or unable to maintain their own computing resources. The need for computing power and storage is ever increasing which is responsible for the increasing popularity of companies which offer cloud services. Clients can easily store and maintain large amounts of data and computation to remote locations, as well as run applications directly from the cloud.

In its early days the members of the cloud community did not all agree on which features should actually be part of the broad concept of cloud computing, the definition that was later provided by the U.S. National Institute of Standards and Technology (NIST) precisely subdivided cloud computing into three distinct service models and four deployment models, which offer differing capabilities to the consumer.

The following definition of cloud computing has been developed by the U.S. National Institute of Standards and Technology (NIST) [16]:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

1.1 Essential characteristics of cloud computing:

There are five main characteristics of cloud computing which include on demand self services, Broad network access, resource pooling, rapid elasticity, measured service and the sixth is multi tenacity.

Services like email, network or server service does not require human interaction with each and every service provider, which is why cloud services are on demand self served. Cloud services are provided over the network so these can be accessed by heterogeneous thin or thick clients like PDA, laptops and mobile phones. The cloud services are used in resource sharing way that is the physical and virtual resources used in these services are not separated for each user but are pooled together make this model more economical. The cloud services often appear to be unlimited as these can be scaled up and down at any time according to the need of user. Cloud services are measured services which have pay per use scenario, client is charged only for the time he/she used the service no charges will be from user when the system is ideal. The resource pooling in cloud computing should be done in a very efficient way, so as even though the resources are shared but the information and data of each client is secure.

1.2 Service Models of Cloud Computing

Cloud computing can be divided into three service models: saas, paas and iaas. Various models can be made by using the combinations of these services depending on the needs.

SAAS (software as a service): provides the infrastructure and software both to the client. The service provider has complete control over the physical settings of cloud and the application capabilities. Thin clients are used for accessing

these applications.

PAAS (platform as a service): in this model the client can create personalized applications using tools provides by cloud service provider. Clients can manage and maintain their applications however; the control of physical settings still remains to cloud service provider.

IAAS (infrastructure as a service): this model provides infrastructure to the client such as (storage, processing and networks). The client is responsible for making operating system and applications on the provides infrastructure.

1.3 Deployment Models of Cloud Computing:

Deployment models are based on the factors like security, customization, where the cloud services are hosted etc. There are four common deployment models Public, Private, community and hybrid cloud.

Public cloud: this model is owned by cloud service provider and is responsible for the security and functioning of this model. All the resources are shared among each other and other organizations and CSP provisions these resources according to need.

Private cloud: this model is solely for a single organization. In this model the organization specifies the security and controls resource pool provided by CSP. Organizations feel more secure using this model as they can enforce their own security rules.

Community cloud: this model is owned by several organizations usually working on a common goal. They share specific needs such as compliance, security etc. Management of this cloud can be done by agencies or CSP and it can be on-premises and off-premises.

Hybrid cloud: this model is simply made by combing two or more other models with a mix of both internally and externally hosted services.

2. Literature Survey

2.1 Zongwei Zhou et. al. proposed a Key management algorithm named as Key it Simple and Secure (KISS). The presented system in this paper protects the life cycle of cryptographic keys. The keys can be used by valid users and applications. Commands can be issued to KISS remotely. It provides protection to system from insider attacks and malware by designing bootstrap protocols using hardware and trusted computing primitives.

2.2 N. Suganthi, V. Sumathy et al., there are three types of keys used in this algorithm. Individual key shared with base station, pair wise key shared with neighbor nodes and group key shared by all nodes. Algorithm is energy efficient uses polynomial function where base station involvement is minimized.

2.3 Ivan Damgård et. al., after studying levels of security on basis of what they can do and what they cannot. Authors proposed protocols for maximal security by considering fully autonomous servers which do not need any assistance while switching between online and offline mode and semi autonomous servers which need little assistance.

2.4 Ramaswamy Chandramouli et. al. reveals that there is additional complexity while managing cryptographic keys in cloud environments. The reason behind this is ownership difference between consumers and cloud service providers along with control of infrastructures on which key management system and protected resources are located.

2.5 Marco Tiloca et. al. Proposed that commonly used time division multiple accesses for communicating in wireless sensor nodes is prone to selective jamming attacks. The presented system SAD-SJ a self adaptive and decentralized MAC layer solution which has limited overhead of communication, energy consumption and computation.

2.6 Md. Monzur Morshed et. al. Proposed a MANET routing protocol cluster based secure routing protocol (CBSRP) for secure communication between mobile nodes. It forms clusters consisting of 4-5 nodes which is energy efficient also. Each cluster has cluster nodes and cluster head which is not permanent and is elected based on the priority. One way hashing is done inside the cluster and digital signature is used for cluster-cluster authentication.

2.7 Seuwou P. et. al. discussed various security issues in Vehicular as hoc network (VANET). VANET makes vehicles into routers which communicate with each other and also with roadside infrastructure. Two broad categorized attacks are done on VANETs; a physical attack occurs due to event data recorder and temper proof device .another is logical attack due to virus, weak spot or Trojan horse.

2.8 Sonam Palden Barfunga et. al, an energy efficient routing protocol based on clustering is proposed in which cluster head is selected by base station. First listing of all nodes which are to become CH is done, then various parameters like relative distance between candidate and BS, remaining energy level, no. of neighbor nodes the candidate has and times for which a candidate node become CH. Further two schedules SLEEP based and TDMA based transmit are created by CH.

2.9 Sajal Sarkar et. al. proposed a trust based protocol which focuses on energy efficiency. It calculated the energy consumption of all sensor nodes and calculates routing metric. Experiments done by author suggest that proposed protocol increases ratio of delivery of packets and reduce delay time.

2.10 Said Ben Alla et. al. proposed energy efficient protocol for heterogeneous wireless sensor networks. It reduced the failure factor of sensor nodes. To increase the lifetime of heterogeneous WSNs the protocol prolongs the time interval of first node's death. High energy cluster heads are elected to collect cluster members information and forward it to gateways.

2.11 XU Jiu-qiang et al., proposed study on WSN topology division and lifetime. Author has increased the connectivity by adding more mobile nodes and a path

planning algorithm is used which reduces effects of connected key nodes. Lifetime of networks is increased by using techniques to discover connected key nodes.

2.12 William B. Davis et al. proposed a junction tree algorithm based on graphical model theory. It is an information processing algorithm which can be instantiated in various applications used in WSNs.

2.13 J. Kusuma et al. Proposed distributed compression for sensor networks. The communication overhead is reduced which is required while to an external observer while preserving data gathering resolution. Data gathering is highly correlating and exploiting it provides more means of compression.

3. 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. A stronger model in a time or situation may a big failure at other time or situation. Usually the key exchange schemes are used between the cloud nodes, cloud platforms and its users to ensure the security of the data being exchanged and to prevent the unauthorized users. During the periods when the Cloud Computing nodes are in working condition, they need secure cryptographic keys for secure propagation of the sensitive information. 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. An effective corporate key management and distribution policy is required to maintain the security of the Cloud Computing platforms along with secure and easy user login & authorization model.

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.

4. Proposed System

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. 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.

5. Conclusion

Cloud security techniques have been frequently used as there is tremendous increase in cloud services. Key management is an important aspect of the cloud security model without it the secure access in cloud computing is not possible.

Several authors proposed various security techniques to be used in the cloud services. This paper has presented a study of various security issues like Client authentication and authorization, Security shortcomings of hardware virtualization, Flooding attacks and denial of service (DoS), Cloud accountability or its ability to capture and expose wrongful activity, Challenges and solutions for remote storage protection.

The new technique is proposed by studying the various papers given in literature review. The proposed work is to design a system Multi-level CK-EAM which will protect entire life cycle of key and allows only authorized user to use these keys thereby solving given security issues.

References

[1] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, “KISS: Key it Simple and Secure Corporate Key Management”, 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, Jesper Buus 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] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, " **Cryptographic Key Management Issues & Challenges in Cloud Services",** Computer Security Division Information Technology Laboratory, NIST, 2013.
[5] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini 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. Monzur Morshed, 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] Sonam Palden Barfunga Prativa Rai, 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] Sajal Sarkar, 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, Moulay Lahcen HASNAOUI, "Hierarchical Adaptive Balanced energy efficient Routing Protocol (HABRP) for heterogeneous wireless sensor networks", IEEE, 2010
[11] XU Jiu-qiang, WANG Hong-chuan,LANG Feng-gao,WANG Ping,HOU Zhen-peng, "Study on WSN Topology Division and Lifetime", IEEE, 2011
[12] William B. Davis, "Graphical Model Theory for Wireless Sensor Networks" (December 8, 2002). Lawrence Berkeley National Laboratory. Paper LBNL-53452.
[13] J. Kusuma, L. Doherty, and K. Ramchandran, Distributed Compression for Sensor Networks, International Conference on Image Processing (ICIP), October 2001.

Authors Profile

Rajesh Kumar Bawa (M.sc., PhD) is currently the HOD of Department of computer science, Punjabi University, Patiala, Punjab, India. He is specialized in the field of Parallel and Scientific Computing.

Jaskarandeep Punia received the B.Tech. degree in Computer Engineering from University College of Engineering, Punjabi University, Patiala, Punjab, India and pursuing M.Tech degree in Department of Computer Science and Engineering, Punjabi University, Patiala, Punjab, India.