IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 2 (Mar. - Apr. 2013), PP 01-06
www.iosrjournals.org

Data Security Model Enhancement In Cloud Environment

Navia Jose[1], Clara Kanmani A[2]
[1](Department of Computer Science, New Horizon College of Engineering/VTU, India)
[2](Department of Computer Science, New Horizon College of Engineering/VTU, India)

Abstract : *Cloud computing is one of the most emerging technologies which plays an important role in the next generation architecture of IT Enterprise. It has been widely accepted due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. In the cloud computing system, both application software and databases are moved to the large data centers, where the data should not be secure in the hands of providers. IT organizations have expressed concerns about the various security aspects that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper describes an enhancement for the already existing data security model in cloud environment. The proposed data security model provides user authentication and data protection. It also ensures fast recovery of data.*

Keyword - *AES Algorithm, Byzantine fault tolerance, Data Security Model, Distributed Denial of Service (DDoS)*

I. INTRODUCTION

With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing, in which resources (e.g. CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion.

In old era of computing, the data and programs are in the hands of the user itself .But with the arrival of cloud computing concept, we can move our data and programs into the provider premises. So the load of users can be decreased to some extent. Cloud computing is the method of computing resources over a network. But the data which ever stored in the provider's hand may not be fully trustworthy. If the provider wants to make any modification in data, they can do it to some extent.

Regarding definition of cloud computing model, the most widely used one is made by NIST as "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].

The cloud computing have major key characteristics. Some of them are:

- Pay as you need–: users to pay for only the resources they actually use and for only the time they require them.
- Highly abstracted –: server hardware and related network infrastructure is highly abstracted from the users.
- Multi-tenant –: multi-tenant architectures allow numerous customer enterprises to subscribe to the cloud computing capabilities while retaining privacy and security over their information.
- Immediately scalable –: usage, capacity, and therefore cost, can be scaled up or down with no additional contract or penalties.
- Measured service-: appropriate metering system is employed and customer's usage of capabilities can be transparently monitored, controlled, and reported.

The cloud computing relies on sharing of resources to achieve coherence and sale similar to a utility over a network.Cloud computing have similar characteristics with other technologies like Autonomic computing, Grid computing, Utility computing ,Client-Server model.

The main objective of this paper is to enhance data security model for cloud computing. The proposed data security model is based on a three layer architecture which solves cloud data security issues by ensuring security in each layer of the model using efficient algorithms explained in this paper.

The paper is organized as follows; in section II cloud computing architecture is defined. Cloud computing security is discussed in section III , in section IV cloud computing security issues are described, and in section V proposed cloud security data model is explained. Section VI focuses on Conclusion. Finally Section VII describes about future work.

II. CLOUD COMPUTING ARCHITECTURE

Cloud architecture model is composed of three service models, four deployment models and seven sub-service models.

1. Cloud Computing Service Models

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

2. Cloud Computing Deployment Models

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[2][19]

3. Cloud Computing Sub-services Models

IaaS: DataBase-as-a-Service (DBaaS): DBaaS allows the access and use of a database management system as a service [12].

PaaS: Storage-as-a-Service (STaaS): STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.

SaaS: Communications-as-a-Service (CaaS): CaaS is the delivery of an enterprise communications solution, such as Voice over IP, instant messaging, and video conferencing applications as a service.

SaaS: SECurity-as-a-Service (SECaaS): SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.

SaaS: Monitoring-as-a-Service (MaaS): MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.

PaaS: Desktop-as-a-Service (DTaaS): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.

IaaS: Compute Capacity-as-a-Service (CCaaS): CCaaS is the provision of "raw" computing resource, typically used in the execution of mathematically complex models from either a single "supercomputer" resource or a large number of distributed computing resources where the task performs well.[2]

III. CLOUD COMPUTING SECURITY

Wikipedia [3] defines Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing."

With cloud computing, all your data is stored on the cloud. So cloud users ask some questions like: How secure is the cloud? Can unauthorized users gain access to your confidential data?

Cloud computing companies say that data is secure, but it is too early to be completely sure of that. Only time will tell if your data is secure in the cloud. Cloud security concerns arising which both customer data and program are residing in provider premises. While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used.

1. Data Security in Existing Cloud Computing System

There are three types of data in cloud computing. The first data in transit (transmission data), the second data at rest (storage data), and finally data in processing (processing data). [2]
Every cloud provider encrypts the data in three types according to table 1.

TABLE 1:Data security (encryption) in cloud computing

Storage	Processing	Transmission
Symmetric Encryption	Homomorphic Encryption	Secret Socket Layer Encryption
AES-DES-3DES-Blowfish-MARS	Unpadded RSA-Elgamal	SSL 1.0- SSL 3.0 – SSL 3.1-SSl 3.2

IV. CLOUD COMPUTING SECURITY ISSUES

There are many security issues associated with existing cloud computing systems and they can be grouped into different dimensions as below.

1. Data Encryption and Integrity Issues

The data stored in the cloud storage is similar with the ones stored in other places and needs to consider two main aspects of information security: confidentiality and integrity.

The common solution for data confidentiality is data encryption. In order to ensure the effective of encryption, there is a need to consider the use of both encryption algorithm and key strength. As the cloud computing environment involving large amounts of data transmission, storage and handling, there also needs to consider processing speed and computational efficiency of encrypting large amounts of data. In this case, for example, symmetric encryption algorithm is more suitable than asymmetric encryption algorithm. [16]

Another key problem about data encryption is key management. Is who responsible for key management? Ideally, it's the data owners. But at present, because the users have not enough expertise to manage the keys, they usually entrust the key management to the cloud providers. As the cloud providers need to maintain keys for a large number of users, key management will become more complex and difficult. In addition to data confidentiality, there also needs to be concerned about data integrity. When the users put several GB (or more) data into the cloud storage, they how to check the integrity of the data? As rapid elasticity feature of cloud computing resources, the users don't know where their data is being stored. To migrate out of or into the cloud storage will consume the user's network utilization (bandwidth) and an amount of time. And some cloud providers, such as Amazon, will require users to pay transfer fees. How to directly verify the integrity of data in cloud storage without having to first download the data and then upload the data is a great challenge. As the data is dynamic in cloud storage, the traditional technologies to ensure data integrity may not be effective.

2. Leakage of Data

While moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Because of them, Data leakage has become one of the greatest organizational risks from security standpoint [5].

3. Attacks in Cloud

Now a days, there are several attacks in the IT world. Internet is the communication infrastructure for cloud providers that use well-known TCP/IP protocol which uses users IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack [7]. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward [8].

Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself. Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact[14]

4. Security Problem Drive from Virtual Machine

For the cloud computing systems the virtual machine technology is considered as a cloud computing platform of the fundamental component. Virtual Machine technology bring obvious advantages, it allows the operation of the server which is no longer dependent on the physical device, but on the virtual servers. In virtual machine, physical change or migration does not affect the services provided by the service provider. If user needs more services, the provider can meet user's needs without having to concern the physical hardware. However, the virtual server from the logical server group brings a lot of security problems.

The traditional data center security measures on the edge of the hardware platform, while cloud computing may be a server in a number of virtual servers, the virtual server may belong to different logical server group, virtual server, therefore there is the possibility of attacking each other ,which brings virtual servers a lot of security threats. Virtual machine extending the edge of clouds makes the disappearance of the network boundary, thereby affecting almost all aspects of security, the traditional physical isolation and hardware-based security infrastructure can not stop the clouds computer environment of mutual attacks between the virtual machine.

5. Consistency of Data

Cloud environment is a dynamic environment where the user's data transmits from the data centre to the user's client. For the system, the user's data is changing all the time. Read and write data relating to the identity of the user authentication and permission issues. In a virtual machine, there may be different users' data which must be strict managed. The traditional model of access control is built in the edge of computers, so it is weak to control reading and writing among distributed computers. It is clear that traditional access control is obviously not suitable for cloud computing environments. In the cloud computing environment, the traditional access control mechanism has serious shortcomings.

6. Attacks from Social Networking

With the increased popularity of business and personal social networking sites the risk of advanced social engineering attacks is increased. Cloud computing systems are targeted due to their large customer data stores. The complex set of relationships between cloud providers, customers, suppliers and vendors means that many employees of these organizations will be listed on social networking sites and be connected to each other. Attacker can setup identities to gain trust, and use online information to determine relationships and roles of staff to prepare their attacks. A combination of technical attacks and social engineering attacks can be deployed against a target user by taking advantage of the people they know and the online social networks they use.

7. Mobile Device Attacks

The use of smart phones has increased and cloud connectivity is now no longer limited to laptop or desktop computing devices. Attacks are now emerging that are targeted for mobile devices .As mobile devices now have these equivalent features .Internet based spyware, worms or even physical attacks may be more likely to occur against mobile devices, as they are potentially a less risky target to an attacker that wishes to remain undetected. This is generally supported by the fact that most mobile devices do not have the equivalent security features enabled, or in some cases available.

V. PROPOSED CLOUD DATA SECURITY MODEL

The proposed cloud security data model is based on a three-layer system structure, in which each layer performs its own duty to ensure the data security of cloud layers.

The first layer is responsible for cloud user authentication. It is designed as OTP authentication module and uses digital certificates issued by the appropriate users and also manage user permissions.

The second layer manages the user's data encryption by using AES algorithm [10], which is the most secured and faster encryption algorithm [2]. For sensitive data such as one's personal information(ex. credit card number) should be encrypted and sent to the cloud .Data integrity is provided by using algorithms like MD5[4] and RSA[6][18]. For non-sensitive data such as one's local information (ex. address details), it should protected by using digital signatures and sent to the cloud. It also protects the privacy of users based on fine-grained attribute based access control policies through access control policy algorithms [9] [20].Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. Such mechanisms should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls [14].

The third layer supports the faster user data recovery by using Byzantine fault tolerance algorithm methods [11] [17] [13].

With three-level structure, user authentication is used to ensure that data is not tampered. The user authenticated can manage the data by operations: Add, modify, delete and so on. If the user authentication system is deceived by illegal means, and malign user enters the system, file encryption and privacy protection can provide this level of defense. In this layer user data is encrypted, even if the key was the illegally accessed,

Through privacy protection, malign user will still be not unable to obtain effective access to information, which is very important to protect business users' trade secrets in cloud computing environment. Finally, the rapid restoration of files layer, through fast recovery algorithm, makes user data be able to get the maximum recovery even in case of damage. [15]

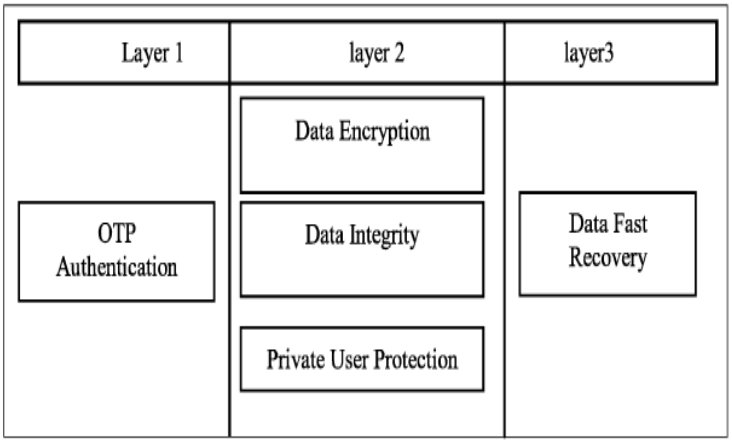

Figure 1.Proposed cloud data security model

Main advantages of the proposed system are

- Highly expressive, fine grained access policies.
- Private user keys with attributes.
- Encrypted files for trusted storage.
- Files can encrypt under policy over attributes.
- Files can be decrypted only if attributes satisfy policy.
- Fault Tolerance System is added.

VI. CONCLUSION

As the development of cloud computing, security issue has become a top priority. The challenges in privacy protection are sharing data while protecting personal information.

This paper discusses the safety issues of present cloud computing data security mechanisms and proposes an enhanced data security model for cloud computing to ensure security in each cloud layers. With the help this new security model, we can improve the security flaws of existing data security model in cloud environment and there by ensuring the data security in cloud environment

VII. FUTURE WORK

For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Proposed model can be enriched by faster data encryption techniques and data recovery

methods. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization

Acknowledgements

The authors would like to thank the anonymous referees for their helpful comments.

REFERENCES

Journal Papers:

[1] Peter Mell, and Tim Grance, The NIST Definition of CloudComputing,Version 15, 10-7-09
[2] Eman M.Mohamed and Hatem S. Abdelkader, Enhanced Data Security Model, The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May, Cloud and Mobile Computing Track, 2012
[3] Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security.
[4] ZhaoYong-Xia and Zhen Ge ,"MD5 Research," Second International Conference on Multimedia and Information Technology, 2010
[5] C. Almond, A Practical Guide to Cloud Computing Security,27 August 2009
[6] Aayush Chhabra and Srushti Mathur, Modified RSA Algorithm - A Secure Approach, 2011
[7] N. Mead, et ai, "Security quality requirements engineering (SQUARE) methodology," Carnegie Mellon Software Engineering Institute.
[8] J. W.Rittinghouse and J. F.Ransome," Cloud Computing: Taylor and Francis Group," LLC, 2010.
[9] Lili Sun, Hua Wang, Xiaohui Tao,Yanchun Zhang and Jing Yang, "Privacy-Preserving Fine-Grained Access Control in Public Clouds, " 2011
[10] K. Cartrysse and J.C.A. van der Lubbe," The Advanced Encryption Standard: Rijndael," Supplement to the books"Basic methods of cryptography" and"Basismethoden cryptografie", October 2004
[11] Joong Man Kim and Yoshifumi Manabe, "A Byzantine Fault-Tolerant Mutual Exclusion Algorithm and its Application to Byzantine Fault-Tolerant Storage Systems, "2005
[12] Cloud Security Alliance Guidance,"Security Guidance For Critical Areas of Focus In Cloud Computing Vl.0",www.cloudsecurityalliance.orglguidance/csaguide.v1.0.pdf, published April 2009
[13] Miguel Castro and Barbara Liskov, "Practical Byzantine Fault Tolerance, "Appears in the Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999
[14] Farzad Sabahi," Cloud Computing Security Threats and Responses," 2011
[15] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan and Tang Chaojing, "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009.
[16] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, 2012
[17] Yilei Zhang, Zibin Zheng and Michael R. Lyu, "BFTCloud: A Byzantine Fault Tolerance Framework for Voluntary-Resource Cloud Computing," IEEE 4th International Conference on Cloud Computing, 2011.
[18] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), 2010.
[19] Center for the Protection of National Infrastructure(CPNI),"INFORMATION SECURITY BRIEFING," March 2010
[20] Mohamed Nabeel, Elisa Bertino," Privacy-Preserving Fine-Grained Access Control in Public Clouds," 2012