Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication

Harpreet Singh,
Research Student,
Department Of Computer Science Engineering,
Chandigarh Engineering College, Landran.

Er. Gagandeep Singh,
Assistant Professor,
Department Of Computer Science Engineering,
Chandigarh Engineering College, Landran.

Er Mandeep Singh,
Associate Professor
Department of Computer Science Engineering,
Chandigarh University, Gharaun.

Abstract— Recent advances have given rise to the popularity and success of cloud computing. However, outsourcing the data to a third party causes the security and privacy issues to become a critical concern. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. In this paper the authors propose to develop private and public cloud, where the private cloud should store only the organization's sensitive structure information such as the key management services and user membership information, and the public cloud should store the actual data in the cipher-text form by using an encryption algorithm where every individual multimedia file will be encrypted using different keys which will be later decrypted by dynamically generating keys at the time of accessing multimedia from Public Cloud.

Keywords-Outsourcing,unauthorized,Encryption, Private, Public, cipher.

I. INTRODUCTION

There has been a growing trend in the recent times to store data in the cloud with the dramatic increase in the amount of digital information or store archival data. Cloud data storage can be particularly attractive for users with unpredictable storage demands, requiring an inexpensive storage tier or a low-cost, long-term archive. By outsourcing user's data to the cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. Cloud can also provide on demand resources for storage which can help service providers to reduce their maintenance costs. Furthermore, cloud storage can provide a flexible and convenient way for users to access their data from anywhere on any device.

The most cited definition of cloud computing is the one proposed by the US National Institute of Standards and Technology (NIST). NIST provides the following definition [1]: "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."

Security issues have been the dominate barrier of the development and widespread use of cloud computing. There are three main challenges for building a secure and trustworthy cloud system:

- **Outsourcing** – Outsourcing brings down both capital expenditure and operational expenditure
for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owners' control.
- **Multi-tenancy** – Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach [2], [3], [4], computation breach [2], flooding attack [5], etc., are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform. Without changing the multi-tenancy paradigm, it is imperative to design new security mechanisms to deal with the potential risks.
- **Massive data and intense computation** – cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

II. LITERATURE REVIEW

Security in cloud is one of the major areas of research. The survey shows that, the researchers are focusing on efficient algorithms and encryption techniques to enhance the data security in cloud. Brian Hay et.al[6] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies and digital forensics. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data. The issues are clarified using the digital forensics techniques namely the ephemeral nature of cloud resources and seizing a "system" for examination. John C. Mace et.al [7] have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions. Service oriented architecture (SOA) is used for work flow deployment in an enterprise. For efficiency, productivity and to achieve public cloud, the cloud computing uses the approaches like retaining control, setting policy, monitoring and runtime security. The dynamic deployment approaches in public cloud computing are security assessment, work flow deployment, policy assignment, audit data and policy analysis. Qiang Guoet.al [8] gives the unique definition for trust in cloud computing and various issues related to trust are discussed here. An extensible trust evaluation model named ETEC has been proposed which includes a time-variant comprehensive evaluation method for expressing direct trust and a space variant evaluation property for calculating recommendation trust. An algorithm based on ETEC model is also shown here. This model also calculates the trust degree very effectively and reasonably in cloud computing environments. Other approaches to protect data privacy in a cloud environment include using direct encryption and proxy re-encryption. In these cryptographic schemes, data is allowed to be encrypted directly to the users with whom the owners wish to share the data [9], [10].

III. PROBLEM FORMULATION

The existing frameworks proposed so far focuses only on securing the data stored either on the distributed servers or local servers interacting with cloud through interfaces or agents. The use of either applying the encryption algorithms or putting the authentication mechanism in place alone cannot help to protect the data from the unauthorized access keeping in view the present robust attacking models. So the need is to suggest such a mechanism where encryption of the content, authorization of user as well the delivery of content to end terminals has been considered.

In a public cloud, as data can be stored in distributed data centers; there may not be a single central authority which controls all the data centers. Furthermore the administrators of the cloud provider themselves would be able to access the data if it is stored in plain format. Hence there is a need of enhancing data security by employing cryptographic techniques to encrypt data from misuse together with some authentication mechanism by which virtue of which the privacy and security of cloud can be achieved on one end and mass data storage feature of public clouds on other end.

IV. PROPOSED 2- WAY AUTHENTICATION MODEL:

In this proposed model the authors will explore the ways to enhance the security of multimedia content using hybrid algorithms while being delivered to their end users. The security frame work will take care of authorization and authentication of user while accessing any cloud server. The hybrid encryption mechanism will make the storage and transmission secure by associating some payloads defining the minimum required security parameters. The robustness of this delivery mechanism will cover the multimedia streaming over CDC, caching the media content onto the edge server from storage cloud and will be used to minimize the latency of content delivery. The overall scenario will outline architecture for designing and deployment of Applications with rich multimedia content over cloud servers as SAAS and also taking the advantage of blob storage of clouds like Windows azure.

First in this proposed model the authors will store all user sensitive information regarding the organization on the private cloud which will not be directly allowed to make interactions with the users. This will help to make the proposed system more secure as there are no accesses for user on that part of storage where our user sensitive information is stored. Next the authors will use the cryptographic algorithm to generate encrypted key and secret key. The encrypted key is used to convert plain text into the cipher-text which is to be later uploaded onto the public cloud. This feature will help any system to use the mass storage concept of public cloud and the use of encryption will serve as an advantage to make it secure from Public Cloud Service provider as well.

In the proposed system the authors are making our system more secure by adding two-way authentication for validating any user for data access. Here first user will be validated for username and password and then later validated in terms of secret key which is already mailed in the mailing account of that user. Moreover in this proposed model the authors will add the subscriptions for users based on their paid memberships. On the basis of this feature the user can access the data with different allocated bandwidths and the different amount of data.

The major outcomes to be achieved in our proposed work are:

- The proposed work is assumed to develop hybrid private cloud and public cloud, where the private cloud should store only the organization's sensitive structure information such as the key management services and user membership information, and the public cloud should store the actual data in the cipher-text form by using any existing encryption algorithm. This proposed architecture not only will dispel the organization's concerns about risks of leaking sensitive structure information, but will also takes full advantage of public cloud’s power to securely store large volume of data.

- In Proposed work all data on public cloud is stored in encrypted form by employing cryptographic techniques which will save data from misuse from cloud service providers and restrict data access to only those intended by the data owners.
- In Proposed Mode, the user is validated using the two authentication mechanism .First the user is authenticated in terms of username and password combination in 3 attempts and then secret key is used for decrypting the original data back into the plain text form. This level two authentication is to be done on per session basis.
- In proposed architecture, User creation will be further made strong by adding premium memberships which will help users to use multimedia resources differently and under different network bandwidths.
- In proposed model while imposing cryptographic techniques, a feature of constant key size needs to be added. Also Revoking User should not affect other users and key management in this architecture.

All these features are summed up in the following flow based figure 1.

V. CONCLUSION:

In this paper, first the authors proposed a new architecture for cloud data storage in which the private cloud should store only the organization's sensitive structure information and the public cloud should store the actual data in the cipher-text form by using newly designed encryption algorithm. The cryptographic algorithm will work on individual multimedia files for which every time the user will have to dynamically decrypt by using different keys. Moreover the authors have proposed the two way authentication for this architecture which will greatly enhance the security of the proposed architecture. The authors believe that the proposed system has the potential to be useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies.

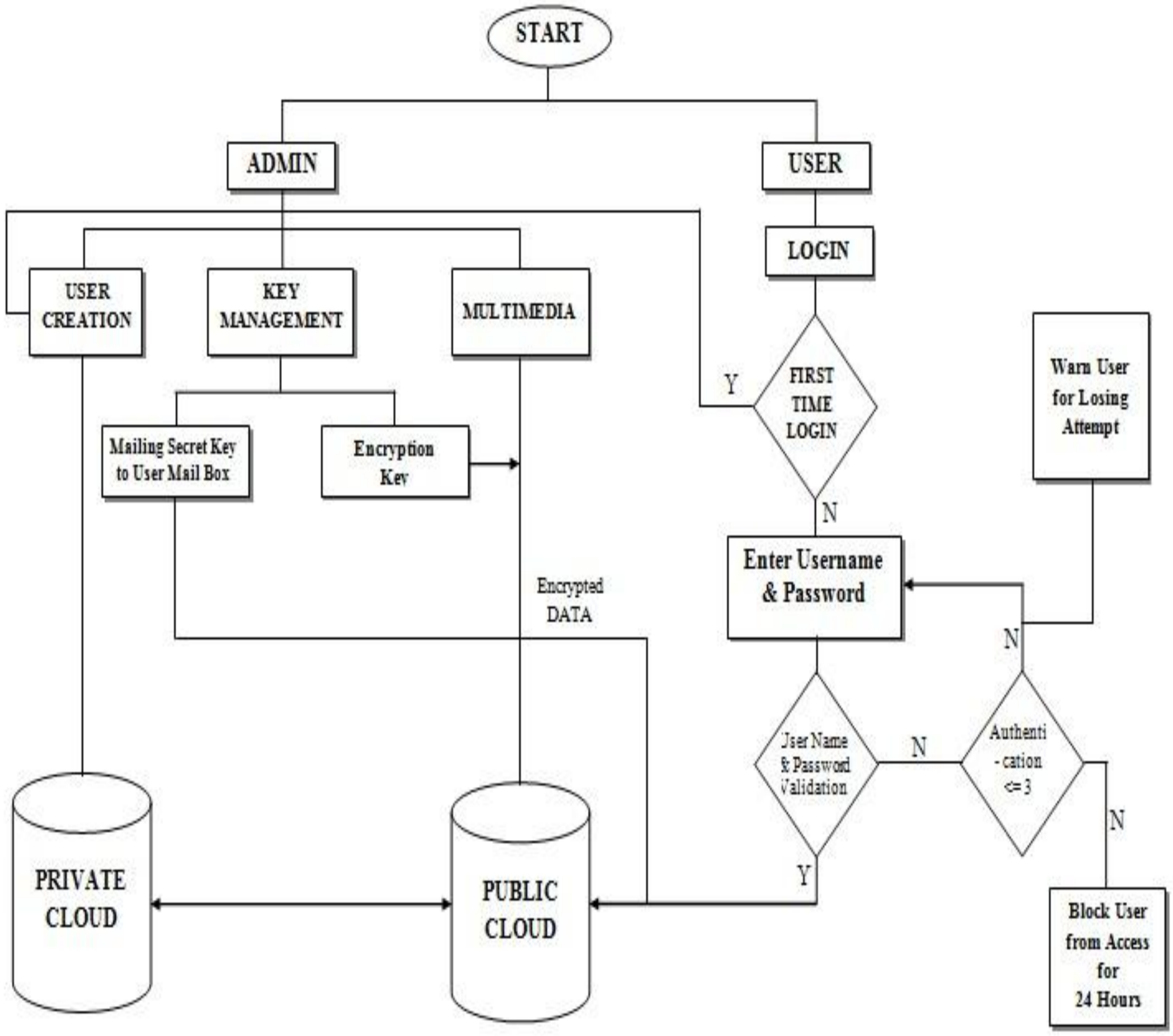
START
ADMIN
USER
LOGIN
USER CREATION
KEY MANAGEMENT
MULTIMEDIA
Y
FIRST TIME LOGIN
N
Warn User for Losing Attempt
Mailing Secret Key to User Mail Box
Encryption Key
Encrypted DATA
Enter Username & Password
N
Jser Name & Password Validation
N
Authenti -cation <=3
N
Y
PRIVATE CLOUD
PUBLIC CLOUD
Block User from Access for 24 Hours

Figure 1 Two-way authentication based Cryptographic model for Secure Data Storage

REFERENCES

[1] P.Mell and T. Grance, “The NIST Definition of Cloud Computing”, 2011.

[2] Google Docs experienced data breach during March 2009. http://blogs.wsj.com/

[3] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, Proc. 16th ACM conference on Computer and communications security, 2009, pp. 199-212.

[4] N. Santos, K.P. Gummadi, and R. Rodrigues,“Towards trusted cloud computing”, Proc. 2009 conference on Hot topics in cloud computing,2009.

[5] C. Dovrolis, P. Ramanathan, and D. Moore, “What do packet dispersion techniques measure?” In Proc. IEEE INFOCOM, pp. 905-914, 2001.

[6] Brian Hay, Kara Nance, Matt Bishop, “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing” Proceedings of the 44th Hawaii International Conference on System Sciences -2011.

[7] John C.Mace, Aad van Moorsel, Paul Watson, “The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments” School of Computing Science & Centre for Cybercrime and Computer Security (CCCS) Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.

[8] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, “Modeling and Evaluation of Trust in Cloud Computing Environments” School of lnformation Science and Engineering, Northeastern University, Shenyang, P.R. China, Computing Center, Northeastern University, Shenyang, P.R. China, 2011 3rd International Conference on Advanced Computer Control (ICACC 2011).

[9] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, “SiRiUS: Securing remote untrusted storage”, in *Proc. NDSS*, pp. 1–15 2003.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,“Improved proxy re-encryption schemes with applications to secure distributed storage” ,in *Proc. NDSS*, pp. 29–43 Feb.