Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Hybrid SecurityModel for Protecting Data in Clouds

Vaibhav Gandhi, Prof. Prashant Lakkadwala
Computer Science & Engineering
Acropolis Technical Campus,
Indore, India

Abstract: In this paper, we present a hybrid model for providing security in cloud computing environment. This model combines the advantages of two most popular existing cloud security model. The first model is hierarchical model and the other one is third party auditor based model. In this paper, we present an overview of existing cloud security algorithms. All these algorithms are described more or less on their own. Cloud security is a very popular task. We describe today's approaches for cloud security. From the broad variety of efficient algorithms that have been developed we will compare the most important ones. At the end, we have also discussed the advantages of the proposed model.

Keywords— Cloud security, HASBE model, TPA model, Cloud computing ,Cloud Architecture

I. INTRODUCTION

Cloud computing [7,8,9] is a internet based network. It is a collection of services. It provides on demand services. The major services provided through cloud are: hardware service, software service, network service. Cloud computing is a modern field, which revolves around utility computing, service oriented architecture, internet, clients etc. Now a days, cloud computing is the heart favourite topic to many researchers. It will become more popular in coming years as the reach of internet is increasing day by day. Cloud computing has three basic models, which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) . The Main advantages of cloud computing are : low cost, improved performance, infinite storage space etc .

II. RELATED WORK

There are many security models for cloud computing. Some popular models are as follows:Attribute-Based Encryption (ABE) was proposed by sahni [1]. It is a fuzzy logic based model. An identity based model was proposed in [2]. It uses the biometric identities for the identification. In [3], Pirretti et al. proposed an efficient model for the large or scalable systems. KP _ABE key policy attribute based encryption was proposed by goyal in [4]. It is an extention of attribute based encryption (ABE)... In [5], Ostrovsky et al. proposed an enhanced KP-ABE scheme which supports non-monotone access structures.

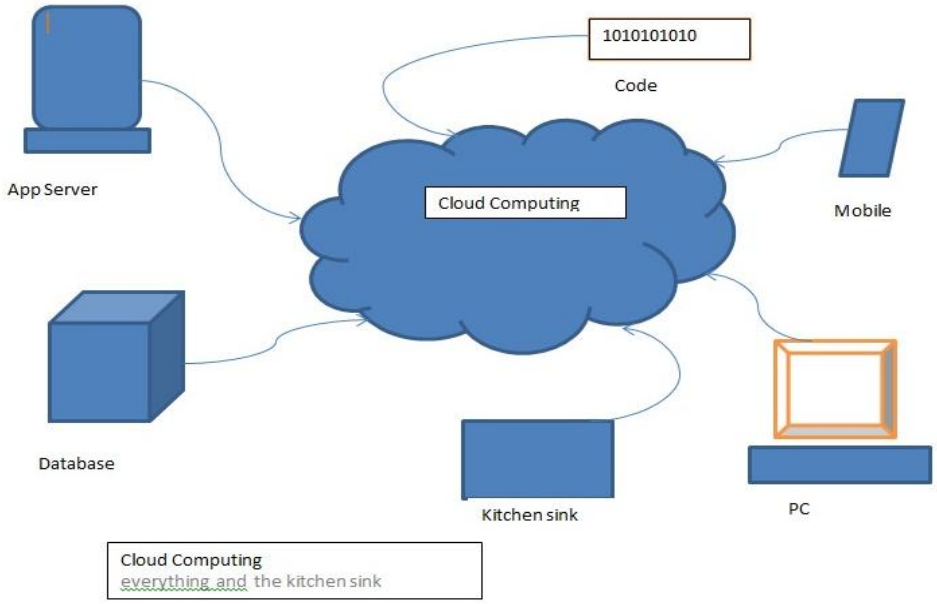

Figure 1: Cloud computing Environment [10]

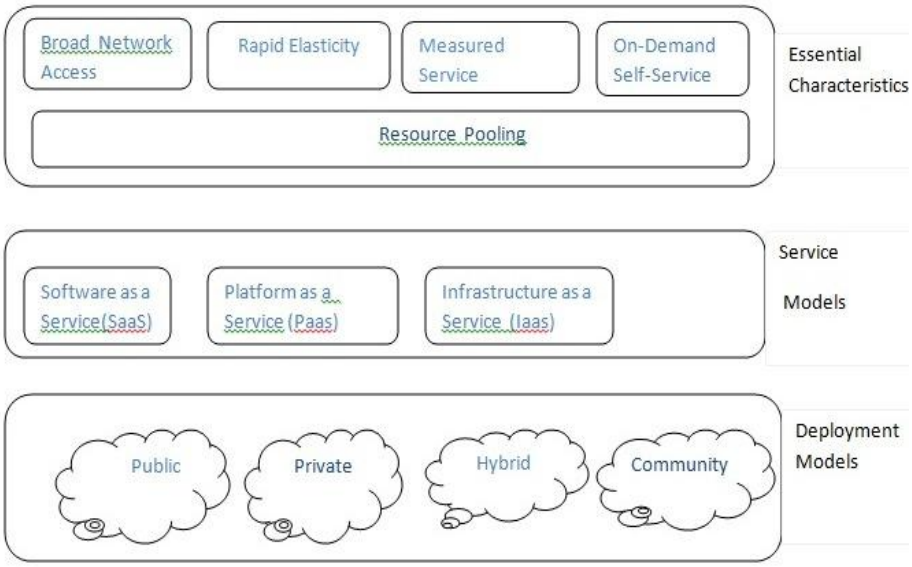

Figure 2: Cloud Architecture [10]

III. PREVIOUS SYSTEM

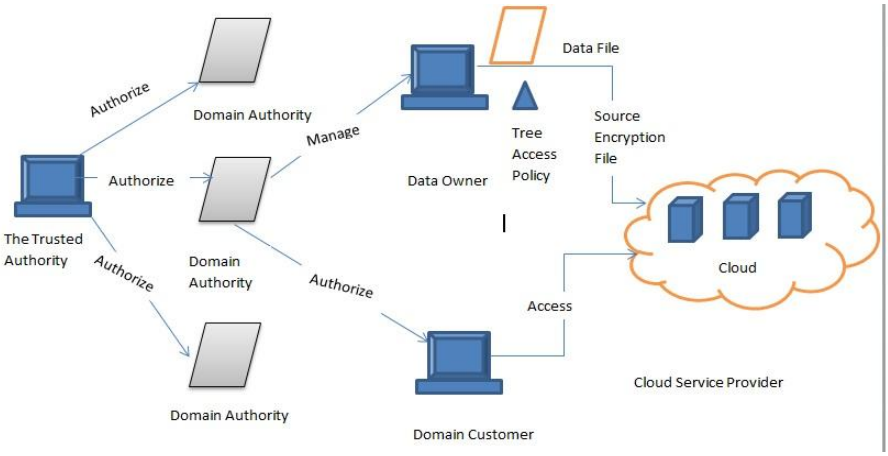

Figure3 : Previous Model [6]

Although the present model overcomes the limitations of the third party auditor based scheme. But it follows a very complex hierarchical structure. We can propose a new model which combines the benefits of both present HASBE model and the third party auditor based model.

IV. PROPOSED SYSTEM

Scheme -1

In our proposed model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. In our model, both data and auditor are present at the cloud servers site.It is responsible for performing functions at all the three layers.

The first layer isUSER AUTHENTICATION

The second layer is DATA ENCRYPTION AND DATA PROTECTION

The third layer is DATA DECRYPTION

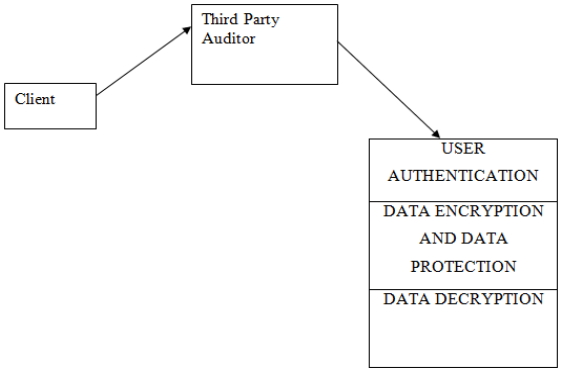

Figure 4: Proposed Model(Schem-1)

Schem-2

Method used in hierarchical attribute set based encryption algorithm for improving efficiency is delegation mechanics. It has capability to share confidential data productively with involvement of full delegation. The delegation is the ability to transfer authority or assigned a third party auditor. The ability of other users to manipulate objects in Active Directoryand also to perform actions on domain controllers and file servers. The delegation defines that it involved for the transfer of authority under server permission. Access control composed of the following components:

- The security point unauthorized user attempt to access resource .
- Authorization data that protects the resource that is being accessed
- An access of user verified that verifies whether requested access can be granted or not.

The process architecture view comprises of the parts of the project work that encapsulates all modules ranging from module to module communication, setting initializations and system. The Delegation is the ability to deal with user's request under the trusted authority's permission. Here the subset of the authority acts as a server for the user. The user no need to wait for the authority until trusted authority gets freed, the request will be delegated to sub authorities when it is busy with other user'.

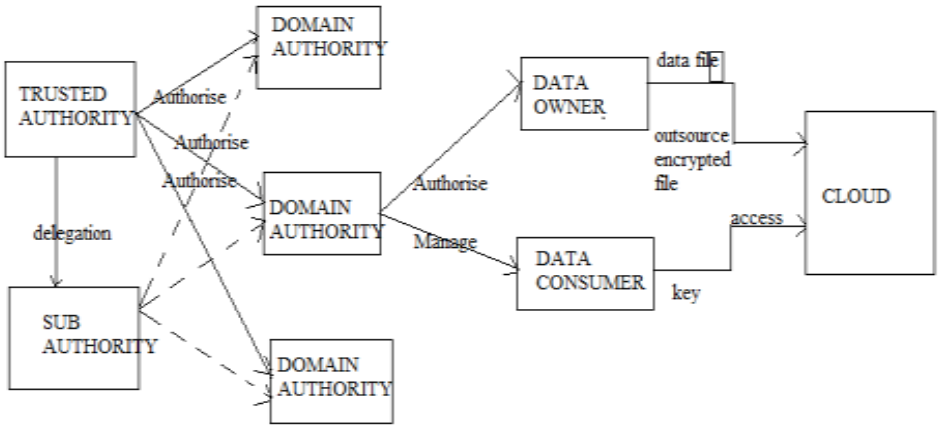

Figure 5: Proposed Model(Schem-1)

The process architecture view comprises of the parts of the project work that encapsulates all modules ranging from module to module communication, setting initializations and system.The Delegation is the ability to deal with user's request under the trusted authority's permission. Here the subset of the authority acts as a server for the user. The user no need to wait for the authority until trusted authority gets freed, the request will be delegated to sub authorities when it is busy with other user'.

V. ADVANTAGES OF THE PROPOSED MODEL

a. Computational Overhead:

In our proposed scheme, the third party auditor and users data is on same site. So the time required for the authentication purpose and data encryption and decryption is less in comparison to previous schemes. In previous schemes, the data and the third party auditor were on separate site. It is clear that in that case the time required for authentication will be more.

b. Authentication Data Security:

In our proposed scheme, the authentication module is playing an intermediates role. Neither the cloud service provider nor the user of the data is able to access the authentication data from it.

c. Scalability:

We extend HASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower-level third party auditor. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability.

VI. CONCLUSION

In this paper, we surveyed the list of existing cloud security techniques. In scheme-1 we presented a new model for the cloud security. It is a hybrid model. It is a combination of the HASBE model and the TPA model. The advantages of the proposed model are Computational Overhead, Authentication Data Security and Scalabilityalso discussed at the end.

In scheme -2 user needs the data to be confidential, even if the cloud service provider is untrusted. The data is to be in encrypted format while storing in the cloud. The existing techniques should not involve in the delegation of the trusted authority. The HASBE scheme provides improved performance of outsourced confidential data but lacks in its scalability and flexibility.One drawback of encryptingdata, is that it can be selectively sharedonly at a coarse-grained level.If trusted authority is busy with another user, the sub authority acts as a trusted authority for the specified user. The authorization has to be delegated for the sub authority to provide required information to the authorized user.

REFERENCES

[1] A. Sahai and B. Waters.Fuzzy Identity-Based Encryption.In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.

[2] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

[3] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data.In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.

[5] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.

[6] Wan, liew "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Controlin Cloud Computing" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012

[7] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[8] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/

[9] Google App Engine [Online]. Available: http://code.google.com/appengine/

