ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Survey on Improved Security in Public Cloud

M.Muthumani[1], Mrs.M.Kavitha[2], Dr.S.Karthik[3]
PG Scholar[1], Assistant Professor[2], Professor and Dean[3]
Computer science and Engineering
SNS College of Technology
Coimbatore, India.

Abstract: Cloud computing is computing paradigm, large number of systems are connected in private or public networks for provide data storage and also file storage because cloud has unlimited storage capacity. Security is protect the data from the unauthorized user access of data. In public cloud security will be implemented by role based encryption, attribute based encryption. All these techniques are related to encryption method. Every data can be encrypted then stored into public cloud so every data has separate encryption key for user identification because more number of users are supported by role based access control. Generally access control consist of authentication, authorization, access approval and also audit. All users assigned by specific roles.

Keywords: Cloud computing, Role Based Access Control, elliptic curves, data storage.

I. INTRODUCTION

Cloud computing is internet based technology, it provide computing resources over the internet. Cloud is the fashionable term for internet and allow the services allow individuals and businesses to use hardware and software managed by third parties. Cloud technology where you go use the technology when you need it, if the internet is available and has no time limit. You pay only for what we use and how to use it. Large number of systems are connected in private or public networks to provide data storage, file storage, scalable infrastructure for application.

A. *Service Models:*

a. *Infrastructure As a Service (IaaS):*

It is the foundation layer of the cloud. This provide additional resources like virtual machine, load balancer, networks, storage, firewalls, images and also videos. Customer can implement their own software on the infrastructure. Supply their resources installed in data center for wide area connectivity.

b. *Platform As a Service (PaaS):*

PaaS providers include combination of OS end application servers and also meet the manageability and scalability requirements of the applications. Application developer develop their software solutions on a cloud platform without any cost and complexity of buying and managing the hardware and software layers.

c. *Software As a Service (SaaS):*

Complete application provide to the customer as a service on demand. Cloud providers install and operate the application software in the cloud. In SaaS cloud users do not manage the cloud infrastructure or platform.

B. *Deployment Models:*

a. *Public cloud:*

The resources are available to the public,, we can utilize anywhere through the internet. All users share the same infrastructure with limited configurations, security protections, availability. Managed and supported by cloud providers.

b. *Private cloud:*

This cloud is operated by single organization by internally or externally. It requires the organization to reevaluate the decisions about existing resources it done right means can improve the business organization.

c. *Hybrid cloud:*

Combination of both public and private cloud is called as hybrid cloud. Cloud providers can fully or partially increasing the flexibility of the computing.

d. *Community cloud:*

Community cloud share the infrastructure between several organizations from a specific community.

e. *Security Issue:*

Security enabled by encryption, protect the data from unauthorized user access of the data.

a) *Detterant control:*

It reduce the attacks on the cloud system. This control reduce the threat level.

b) *Detective control:*

In this any event or incident occurred means detective control signals the preventive or corrective control, it detect and react appropriately. Detect attacks on cloud can control by hardware or software security monitoring, intrusion detection.

c) *Preventive control:*

Strength the cloud system by less likely unauthorized user access and more likely cloud users are positively identified.

d) *Corrective control:*

It reduce the consequences of an incident by limiting the damage. Example: restoring the system backups inorder to rebuild the compromised system.

In this paper RBE allows Role Based Access Control for secure data storage mentioned in[1]. In public cloud RBAC[1] allows more number of users to store and access the data. Unauthorized users are also allowed to this process so we think the data cannot be secured. But in RBAC initially encrypt the data then only store into the cloud so any user can store or retrieve the data necessary to know the private key of that data. Because each and every data has single private key for encryption.

Any problem arises in key management means access policies used to determine that problem. These policies are defined as each user can satisfy some access policies mentioned in [1].Large volume of data stored in cloud and also be secured but the decryption time will be worst as [4] so performance also degraded.

RBE Architecture

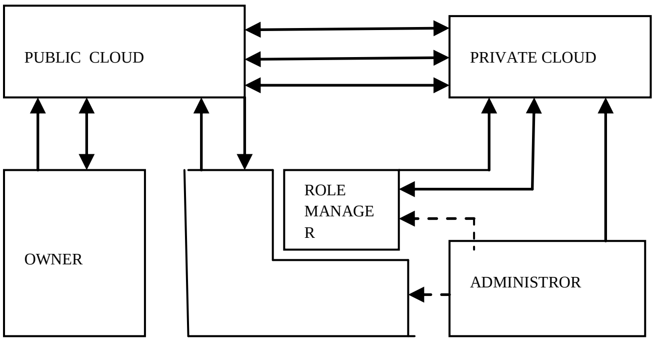

Figure: 1

II. LITRATURE SURVEY

A. Achieving Secure Role Based Access Control:

RBE allows RBAC(Role Based Access Control) [1].It consider hybrid cloud architecture here private cloud maintain sensitive information. But public cloud more number of data, only authorized person can store and retrieve the data from public cloud. So small amount of data only stored and also not securable. Now RBAC restrict the authorized users it allows more number of users to store large amount of data in public cloud. Here private cloud users not allowed to store or retrieve the data from public cloud. If more number of users allowed so we think data is not securable. But RBAC introduce encryption algorithm[1], initially all the data can be encrypted then only stored into public cloud. Each and every data has particular single encryption key. In this paper decryption time will be more because of more number of users processed so performance also use elliptic curve characteristics.

B. Enforcing Rbac For Secure Data Storage:

RBE introduce broadcast encryption algorithm describes the security. It proposed the hybrid scheme that combines access control with cryptography and key distribution to provide security requirements and overcome the KP-ABE [6]. In KP-ABE owner of data not have to control who allowed to access the data. Normally cryptography with RBAC simplify the security concerns. In RBE each and every data can be assigned with specific role by role manager. User join with role after data owner encrypt the data. User can be invalidate from the task without affecting the data owner and also same user of the same task. ABE [6] cipertext labled with set of attributes, this set of attributes are combined with policies contains CCA secured solution and also constant size as [4]. Data owner only decide to encrypt the data based on which user can satisfied the roles are specified by RBAC.

C. Role Based Encryption With Revocation Mechanism:

Previous cryptographic systems are not support for processing the large number of users. Interoperability and role based access control capabilities also not supported by existing one. So introduce role based cryptosystems it provide the security concerns like key encryption, signature and authentication based on role hierarchy. Here RBE assigned permissions and roles to the private keys and cipertexts. This cryptosystem different from others because of RBE[1],[2]provide encryption algorithm to group of users. Dynamic user revocation method describe the key hierarchy it supports partial ordering and bilinear maps. RH has achieved better performance and scalability. This system not fully support for the process of practically large number of organizations.

D. Identity Based Encryption:

CCA (chosen ciper text attacks) [4] secure public key cryptosystem and IBE- Identity based encryption[5] has been introduced. It is flexible compared to Kurosawa and desmedt because of security proof and effectiveness. Hybrid encryption has to be introduced; it contains both public key encryption and symmetric key encryption. Public key encryption contains triplet form(Gen, Enc, Dec).IBE related to public key encryption, this scheme in which any string can act as public key for encryption. IBE contains 4 tuples (setup, derivation, Enc, Dec). Authentication algorithm take key and message M as input. Verification verify the output is 0 or 1. The output is 0 rejected if 1 means the output can accepted. Here decryption time is worst to solve this problem implement the proposed scheme.

E. Public Key Encryption With Keyword Search:

Public key system introduced to search the encrypted data. Example: Mail server that store different type of messages these are publicly encrypted. Private database and public dsatabase are maintained. In private database user upload data to remote database and stored in remote database administrator, data can be recover with particular keyword. In public database data is available to public user want to think retrieve some data but finally retrieve some other data. To avoid this problem use public information retrieval protocol (PIR). Public key encryption is related to identity based encryption. Any string acts as public key.

F. Attribute Based Encryption:

In attribute based encryption implement key policy attribute based encryption for the purpose of overcome the some problem in data storage. More sensitive information can be stored by third parties to overcome this introduce KP-ABE [2]. It refers each and every cipertext has associated with set of attributes and also private keys. Private keys are associated with secure control structure.

III. METHODOLOGY

Existing consist of hybrid architecture, private cloud already maintain sensitive information only stored so the data has securely stored. But in public cloud not like that the resources are available to public the data is unsecured and allow particular users. But proposed method refers role based encryption to restrict limited users it permits more number of users after encryption only data stored or retrieve from public cloud. Every data have separate encryption key for identification and also security purpose. Here decryption time will be more so performance also reduced.

To overcome this problem implementing elliptic curve characteristics performance also increased.

IV. CONCLUSION

In this paper make survey on large amount of data can be securely stored into public cloud. Then access control mechanisms like role based access control are discussed. RBAC support more number of roles it refers multiple techniques and encryption algorithms for improving performance from above related survey. Further implement more cryptosystems to increase the security in cloud. Because cloud is recent emerging technology and very useful to many large organizations because of it unlimited data storage space.

V. REFERENCES

[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens ”Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage” IEEE transactions on information forenics and security, vol. 8, no. 12, Dec 2013.

[2] L.Zhou, V. Varadharajan, and M. Hitchens, “Enforcing role-based access control for secure data storage in the cloud,” Comput. J., vol. 54, no. 13, pp. 1675–1687, Oct. 2011.

[3] Y. Zhu, H. Hu, G.-J. Ahn, H. Wang, and S.-B.Wang,“Provably secure role based encryption with revocation mechanism,” J.Comput.Sci.Technol., vol. 26, no. 4, pp. 697–710, 2011.

[4] D. Boneh and J. Katz, “Improved efficiency forCCA-secure cryptosystems built using identity-based encryption,” in CT-RSA (Lecture Notesin Computer Science), vol. 3376. New York, NY, USA: Springer-Verlag, Feb. 2005, pp. 87–103.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, andG.Persiano,“Publickey encryption with keyword search,” in EUROCRYPT (Lecture Notes in Computer Science), vol. 3027. New York, NY, USA:Springer-Verlag, 2004, pp. 506–522.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters,“Attribute-based encryption for fine-grained access control of encrypted data,”in Proc. ACM Conf. Comput. Commun. Sec., Oct./Nov. 2006.