ISSN (Online): 2455-7838
SJIF Impact Factor (2015): 3.476

EPRA International Journal of

Research & Development

(IJRD)

Volume:1, Issue:4, June 2016

Published By :
EPRA Journals

SJIF Impact Factor: 3.476 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 1 | Issue: 4 | June | 2016

A COMBINED APPROACH FOR SECURING CLOUD USING AES ALGORITHM & AGGREGATED KEY CRYPTOSYSTEM

Faizan Ahmad[1]
[1]PG Scholar, Department of Computer Technology, KITS, Ramtek, Maharashtra, India.
S.V Hemant[2]
[2]Assistant Professor, Department of Computer Technology, KITS, Ramtek, Maharashtra, India.

ABSTRACT

Data sharing is one of the important aspects of cloud storage. In this paper we show how to share the data with the others in cloud storage in a secure and efficient manner. We are proposing new public key cryptosystem that produces constant size cipher texts such that it authorize and delegate the decryption rights for any set of cipher text. The specialty of this system is that it aggregate any set of secret keys and make it compact single key that posses the power of all keys. This compact aggregate key can be efficiently sent to others. For the encryption we are using AES algorithm which is one of the most powerful encryption. By combining the AES algorithm and KAC algorithm we are making the system more efficient and the problem of key management will be reduce. Main objective of this paper is to store data securely in cloud storage and maintaining the security while accessing the data.

INDEX TERM: *Cloud storage, data sharing and key aggregated encryption*

I.INTRODUCTION

There is no concern about the fact that cloud computing has been growing day by day. Companies all over the world are tuning to different cloud platform for their I.T needs. It is the fact that, 80 % of assets of 1000 companies was used various aspect of cloud computing in the year 2013 & 20% do so without buying single piece of hardware.

How cloud computing will define? The national institute of standards and technology gives definition: The cloud enables convenient ,on demand network access to a giving pool of computing resources-networks, servers, storage applications, and services among others several key features are crucial to the cloud offering and to today's dynamic business environment. Cloud computing fails in some security measures the threat to the security of clouds is data theft attacks. Data sharing is one of the important aspects of cloud storage. In this paper we show how to share the data with the others in cloud storage in a secure and efficient manner.

We are proposing new public key cryptosystem that produces constant size cipher texts such that it authorize and delegate the decryption rights for any set of cipher text. Here we are using Microsoft azure as cloud storage and AES algorithm for the encryption. Data which is going to be share is divided into four parts using simple random sampling after that there is key generation using auto key generation. By using this key encryption is performed and data is going to be encrypted which is going to be store in different containers of cloud storage. Now if authorize user wants this data than data owner give Master secret key that posses the power of all keys to that legal user now this Master secret key will be enter by the legal user than automatically data is merge from

different cloud storage containers and it is going to be downloaded by the legal user. In this way data is going to share in secure manner without losing confidentiality of data which is our main objective.

A. Features of cloud computing:-

Cloud computing is defined by five features

- On-demand self service: Establish manage and terminate services on your own, without involving service provider.
- Broad network access: Use a standard browser for accessing the interface, without any software adds-on or specific operating system requirement.
- Resource pooling: Share resources and cost across large pool of users, allowing for centralized and increased peak load capacity.
- Rapid elasticity: Enhance capacity as needed, if it is needed then give it back when it is no longer required.
- Measured services: Consume resources as service and pay only for resources use.

B. Service models of cloud computing:-

Various service models of cloud computing are:

a) Software as a Service (SaaS): In a Software as a Service model pre-made applications, along with any operating system, software, hardware and network.

b) Platform as a Service (PaaS): In a Platform as a Service model user can develop his own software and applications. Basically it provides platform to develop various software and applications.

Infrastructure as a Service (IaaS): In Infrastructure as a Service user can develop or install his own operating system, software and applications rather than purchasing servers, network devices, etc.

C. Deployment models of Cloud computing:-

The deployment models of cloud computing are categorizes according to their accessibility, structure of organization and provisioning location. They are:

a) Public cloud: Public cloud is totally depend upon standard cloud computing infrastructure in which service provider makes all the resources available to general public over the internet.

b) Private cloud: Private cloud is owned by an organization which is hosted externally or internally and manages internally or by trusted third party. Private cloud can only access by members, employs and trusted third party of organization.

c) Community cloud: In community cloud the infrastructure is shared among several organization from some of community which handled it internally or by third party and also host internally or externally.

d) Hybrid cloud: Hybrid cloud is the combination of public, private or community clouds.

II. MICROSOFT AZURE

Microsoft Azure provides a Microsoft Windows Server based computing environment for applications and permanent storage for the data, as well as asynchronous messaging. Azure also provides a range of services that helps us connect users and applications to cloud-hosted applications, manage authentication, use main services of messaging, and execute management of data and related features such as caching.

Azure also includes a range of management services that allows us to control all these resources, either through a web-based user interface or by using programs. In most of the cases there is a REST-based API that can be used to define how our services will work. All the management tasks that can be performed by the web portal can also be performed by using the API.

COMPUTING ENVIRONMENT OF MICROSOFT AZURE's:

The computing environment consists of a platform for applications and services hosted within one or more roles. The types of roles we can implement in Azure are:

Azure Compute(Web and Worker Roles). Microsoft Azure application consists of more than one hosted roles that are running within the Azure data centers. Typically there will be at most one web role that is shared for access by users of the application. A web role is supported by Internet Information Service and also by ASP.NET. Either application may contain additional roles or worker roles, that are use to perform backend processing and helping tasks for web roles.

Virtual Machine (VM role). This VM role allows to host our own customize SERVER that incompases Standard operating system within an Azure data center.

DATA MANAGEMENT IN MICROSOFT AZURE

Azure, SQL Azure, and the associated services provide advantages for the storing and the management of the data in a different ways. The following data management services are:

- **Azure Storage**. It provides more than one core services for persistent and durable data storage in the cloud. The four storage services are listed below:

1. **The Azure Table Service:-** The Azure Table Service provides structured-table storage management and queries for managing the data. The Azure Table Service is a Not SQL that provides less storage in concern of the schemas. Its main aim at scenarios where large volumes

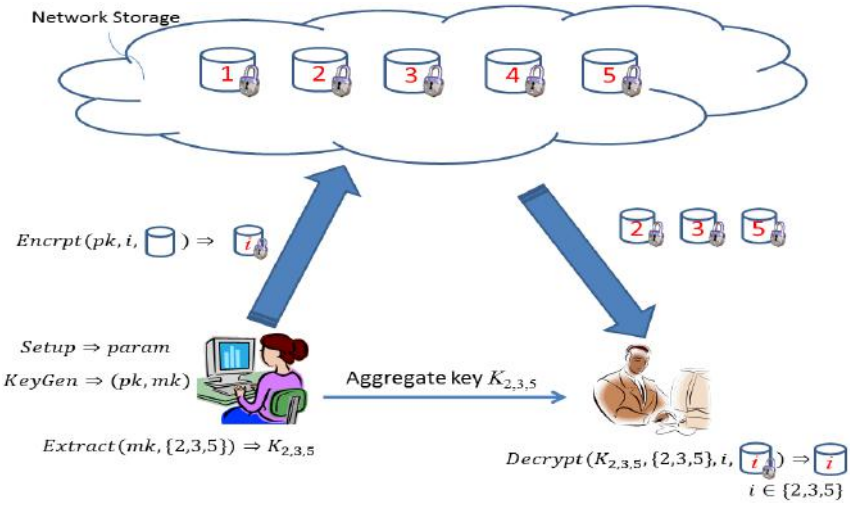
of data must be stored, while being easy to access and update.

2. **The Binary Large Object (BLOB) Service:-**The Binary Large Object (BLOB) Service provides different of containers that storing simple text or binary data. It provides both Block BLOB containers for processing of data, and simple pages BLOB storage containers for simple read/write operations.
3. **The Queue Service:-** The Queue Service provides a mechanism for reliable, persistent messaging between role instances, such as between a web role and a worker role.
4. **Azure Drives:-**Azure Drives provide a mechanism for applications to mount a single volume NTFS VHD as a Page BLOB, and upload and download VHDs via the BLOB.
   - **SQL Azure Database**. It is a mostly available and efficient database cloud services that built on SQL Server technologies that supports the familiar T-SQL-based relational database model. It is jointly used with applications that hosted in Microsoft Azure, and with other applications running on-premises or hosted elsewhere.
   - **Data Synchronization.** SQL azure Data Synchronization is a cloud-based data synchronization service built on Microsoft Synchronization infrastructure technologies. It provides two directional data synchronization and data management capabilities, allowing data to be easily access between several SQL azure databases and between on-premises and SQL azure databases.
   - **Caching**. This service provides a hierarchical, within memory, low bandwidth and high throughput application cache service that neither requires any installation or management, and it is radically increases and decreases the cache size as required. It can be used for caching the application data, ASP.NET session state information, and for ASP.NET, page output caching.

III. KEY AGGREGATE ENCRYPTION (KAC)

Initially we describe the main components of KAC than we describe the application of KAC in cloud storage.

- **Components of KAC:-**KAC scheme will have five algorithms that run in polynomial time. Data owner will maintain the public system parameter through Setup which generates pair of public key/Master secret key through KeyGen. Encryption of messages done by Encrypt function by everyone or data owner and also decides which cipher text class is encompasses with the plaintext message which is going to be encrypted. Owner of the data will use master secret key to generate an aggregate decryption key for a particular set of cipher text classes through Extract. Now the keys are passed to delegates in secure manner at last any user with an aggregate key can decrypt any cipher text through Decrypt.
  i. Setup: - It is implemented by the owner of data to setup an account on non trusted server.
  ii. KeyGen: - It is implemented by the owner of the data to generate Public/Master secret key pair.
  iii. Encrypt: - It is implemented by anyone or data owner who wants to encrypt data.
  iv. Extract: - It is implemented by the data owner for giving decrypting power for particular set of cipher text classes to whom that want to access this data.
  v. Decrypt: - It is implemented by the user that received aggregate key through Extract.
- **Application of KAC in Cloud Storage:-**



• **IMPORTANT STEPS:** - Following are the important step which perform during accessing of cloud server

1.Authentication And Authorization
2.File Encryption by KAC
3.Cloud data sharing
4.File Decryption by KAC
5.Regeneration of Data

1.Authentication and Authorization:- These process are the required of the Verification the User Originality and Appropriate Session Activities of the Registered User.

2.File Encryption by KAC: - After user login, the user can able to store the files into the cloud in an encrypted form. The encrypted data which are stored in the cloud cannot be decrypted normally by other users or hacker's.

3.Cloud data sharing: - The user initially uploads's files data to the cloud, and shares it with other users. The shared files are encrypted by the owner. Whenever the other user's want to access or decrypt the file required key permission to be provided by data Owner.

4.File Decryption by KAC: - The aggregate keys are sent in mail to other user by the original user. The file will be decrypted by the aggregate key's which was generated by the KAC. Finally, any user with an aggregate key can decrypt any cipher text.

5.Regeneration of Data: - In Case of Corruption of any Share of data or loss of any share on cloud, that particular share will be regenerated from a backup storage.

IV. ACKNOWLEDGMENT

I would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

V. CONCLUSION

Data privacy is one of the most important aspects of the cloud storage. There are several mathematical tools and cryptographic technique that involve several keys for single. In this paper our main focuses is on how to compress secret key in a public key cryptographic environment that support delegation of secret keys for the different classes of cipher text in cloud storage also the person that want to access to the particular data will get constant size aggregate key. Our method is more convenient than the hierarchical key assignment scheme that can only reduce spaces if all the holders of key share a similar set access. Limitation of this method is the predefined bound of the number of cipher text classes as in cloud storage the number of cipher text are increases rapidly.

VI. REFRENCE

1. *Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng Senior Member, IEEE key –Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage IEEE Transactions on Parallel and Distributed Systems. , 25(2) , 468.2014*
2. *C Wang, S.S.M.Chow, Q.Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013*
3. *S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications – Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464*
4. *M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol.12,no. 3, 2009.*
5. *V.Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, "in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.*
6. *D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT 03, ser. LNCS,vol. 2656. Springer, 2003, pp. 416–432*