Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.64 – 69

RESEARCH ARTICLE

Analysis of Attribute Set-Based Encryption Solution for Access Control in Cloud Computing

P. Sravanthi[1], N. Uday Bhaskar[2], P. Swapna[3], Nagaraju[4]

[1]M.Tech, Computer Science Engineering, Vijay Rural Engineering College, India

[2]M.Tech, Computer Science Engineering, Sri Indu College of Engineering & Technology, India

[3]Associate Professor, Computer Science Department, Vijay Rural Engineering College, India

[4]Assistant Professor, Sri Indu College of Engineering & Technology, India

Abstract— Cloud computing is one of the most influential domain in the information technology. Encryption scheme perform sequence implicit operation on the plaintext by processing the original text which supports all the operations increases the storage capacity and provides the secure data transfer. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption by extending cipher text-policy attribute-set-based encryption with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of attribute set-based encryption. Hierarchical attribute set based encryption employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of hierarchical attribute set based encryption based on security of the cipher text-policy attribute-based encryption scheme. We also present comparison on encryption our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive analysis.

Keywords: - Encryption; Cryptography; Hierarchical Attribute Set-based Encryption; Cloud Computing

I. INTRODUCTION

The compelling Advantage moving to the cloud reduced cost grater scalability increased mobility fast deployment and instant updates to a novel data privacy residency security and compliance risks continue to be the primary hurdle for cloud adoption by enterprise organizations. The Cipher cloud platform eliminates these risks by delivering a single platform to secure sensitive customer information across all cloud applications while preserving usability functionality and performance. Cipher cloud delivers a comprehensive set of protection controls encryption

The Cipher cloud gateway incorporates a number of military grade AES based format operations preserving encryption schemes that can be used to secure cloud data before it leaves the enterprise network while preserving the usability and functionality of cloud applications. Organizations are able to reap all the benefits of migrating to the cloud without to manage the overhead of storing sensitive data in local databases. The ability to select from various encryption schemes on a field by field basis provides customers the granularity needed to comply with their organizational data classification and regulatory requirements. Cipher cloud has implemented strong software based cryptograph key management standard NIST SP 800-21 that includes key rotation split custodians key encrypting keys and many other capabilities. Cipher cloud gives you a control point for corporate

© 2013, IJCSMC All Rights Reserved

data going to and from the cloud users internal remote or mobile can seamly access sales force cloud applications while enabling you to enforce organization security policies. The process is transparent to authorized users to preserve the functionality of sales force cipher cloud provides AES 256 encryption tokenization cloud data loss prevention cloud malware detection.

Cloud encryption is more secure by ensuring that data remains being processed, schemes Homomorphic encryption Garbeled circuit and attribute based encryption into what a call functional encryption scheme according to a report in research center. A scheme that keeps data secure every step of the way would likely appeal to public sector agencies which are increasingly moving applications and services to cloud systems although which are increasingly moving applications and services to cloud systems although for the foreseeable future have to rely on current security scheme requires more than would be practical.

II. RELATED WORK

The survey of major cloud service providers to investigate the security mechanisms to overcome the security issues discussed in this paper. We consider ten major cloud service providers. These providers provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. List shows the list of service providers that we studied in this survey. In order to analyze the complete state of art of security in cloud computing, the survey needs to be more exhaustive. However, due to the fact that the scope of our work is not just to explore the state of art but to look at the major factors that affect security in cloud computing. Therefore we have intentionally not considered other cloud service providers in this survey. In list 2, we present the results of the survey that depicts the current state of security mechanisms. Information given in table 2 is based on the information available online at the official websites of these providers.

1. IaaS Service Provides is an Amazon EC2 Amazon S3 Go Grid
2. PaaS Service Provides Google Application Engine Microsoft Azure Services, Elastic Map Reduce
3. SaaS service provides Sales force Google Docs

Security Issues on Cloud Computing

Password Recovery 90% is using standard methods like other common services while 10% are using sophisticated techniques.

Encryption 40% are using standard SSL encryption while 20% are using encryption mechanism but at an extra cost 40% are using advance methods like HTTPS access

Data Location 70% have their data centers located in more than one country while 10% are located at a single location 20% are not open about this issue.

Cloud computing is a model for information and services using exiting methods, it uses the internet infrastructure to allow communication between client side and server side applications. Cloud clients service providers provides exist between that offers cloud platforms for their customers to use and create their own web services. When making decisions to adopt cloud services privacy or security has always been a major deal with these issues the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used.

The major security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management [3],various security issues arises in cloud computing.

Top seven security threats to cloud computing discovered by “Cloud Security Alliance” (CSA) are [4]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

A solution that works well in an Infrastructure as a Service cloud may not work well in SaaS Software as a Service cloud environment similarly there are many considerations to transparency of solution and ease of management there are also issues related to who owns manages to access to encryption keys. This provides a high level overview of encryption options and categories of available solutions in different scenarios. Many options for encrypting data in cloud which may have some trade-offs at a high level.

Disk encryption is available for clients with full access to the operating system

© 2013, IJCSMC All Rights Reserved

File encryption is achieved either using native operating system or by installing an agent to enforce encryption policy.

Database encryption field or table view can be achieved in many ways in the cloud solutions are available from major database vendors as well as third parties. Encryption gateways can also for database encryption. Third party solutions work by intercepting JDBC/ODBC procedures.

Encryption based solutions are available from multiple vendors for cloud environment encryption is placed between the cloud environment and private network data centers to encrypt decrypt data in real time.

Hypervisor encryption solution enables IaaS customers to run another virtualization layer to implement encryption at hyper level.

Tackle Before Encrypting Cloud Data: The annual growth of Software as a Service from 2011 is 19.5% platform as a Service 27.7% Infrastructure as a Service 41.3% however security cited by many organizations as the top inhibitors of cloud services adoption which has led to the introduction of cloud encryption system in the past. Encryption is the enterprises first develop data security plan that addresses security issues.

Breach Data Residency: For all data requires equal protection so business should categorise data intended for cloud storage and identify any compliance requirements in relation to data breach. Enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities such as legal contract business units security and information technology.

Data Management:

To determine business specific cloud service providers data storage security policy

Multitenant storage is being used and find out separation mechanism is being between tenants.

Multitenant such as tagging are used to prevent data being replicated to specific countries

Storage used for archives and backup is encrypted and if the key management strategy includes a strong identify and access management policy to restrict access within certain jurisdictions.

Data Protection in cloud is business ensure that the CSP will support secure communication protocols such as SSL TLS browser access or VPN based connections for system access for protected access to their services. Enterprise should always aim to manage the encryption keys but if they are managed by a cloud encryption provider Gartnet says must ensure access management controls are in place that will satisfy breach requirements and data residency. If keys are managed by the CSP then business should require hardware based key system within a defined set of processes. Access controls Gartner recommends that businesses require the CSP to support IP subnet access restriction policies so that enterprises can restrict end-user access from known ranges of IP addresses and devices. The enterprise should demand that the encryption provider offer adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network and maintenance. Businesses should also requires as follows Logging of all user and administrator access to cloud resources, and provide these logs to the enterprise in a format suitable for log management or security information and event management systems. The CSP to restrict access to sensitive system management tools that might "snapshot" a live workload, perform data migration, or back up and recover data. That images captured by migration or snapshotting tools are treated with the same security as other sensitive enterprise data.

III. PROBLEM DEFINITION

3.1 Problem Definition: Cloud computing relies on sharing computing resources rather than having local servers or personal devices to handle applications and used as a metaphor for the internet so the phrase cloud computing means a type of internet based computing. To apply traditional supercomputing or high performance computing normally used by military and research to perform such as financial portfolios to deliver personalized information to provide storage or to power large uses networks of large groups of servers.

Cloud computing provides clients with a virtual computing infrastructure on which they can store data and run applications, introducing new security challenges since cloud operators are expected to manipulate client data without necessarily being fully trusted.

Cloud computing provides cryptography even in order to realize scalable flexible and fine grained access control of outsourced data, we analyze encryption methods and priority hierarchical structure of users.

Encryption is the conversion of data into a form called a cipher text that cannot be easily understood by unknown persons and decryption is the process of converting encrypted data return into its original form. Use of encryption/decryption is art of communication cipher often incorrectly called a code can be employed to keep the enemy from obtaining the contents of transmissions. In order to easily recover the contents of an encrypted signal the correct decryption key is required alternatively a computer can be used in an attempt to break the cipher. Fact that encryption might be accidently utilized on something that was not meant to be encrypted and the person who was meant to obtain the message may not be able to read the message sent to them, may not be

© 2013, IJCSMC All Rights Reserved

strong enough and therefore others may be able to easily interpret information. Hierarchical structure of system users to achieve scalable flexible and fine grained access control low initial capital investment and maintenance.

3.2. Analysis for the above Problem: Cloud server is either proportional to the number of system attributes or linear to the size of the user access structure tree achieved. Our construction also protects user access privilege information again cloud server.

Method for Hierarchical Attribute Solution:

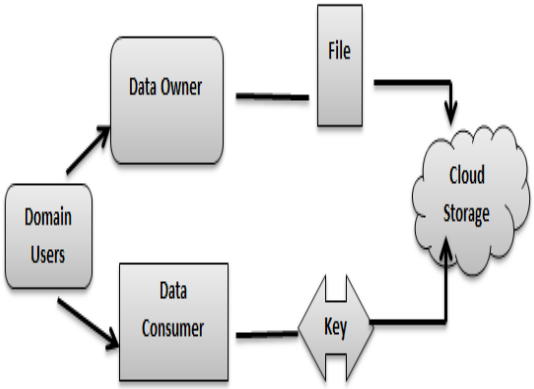

Figure 1 Proposed System

Data owner uploads the data in the cloud server for the security purpose, owner encrypts the file and store in the cloud and owner as rights to change the policy over data files by updating the expiration time.

Data Consumer user can only access the data files with the encrypted key if the user has the privilege to access the file. For all user level all the privilege is given by the domain authority and the data users are controlled by the domain authority.

Cloud service provider manages a cloud to provide data storage service, data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files data consumer download encrypted data files.

Authority person is responsible for generating and distributing system parameters and root master keys as well as authorizing the high level domain authorities. Domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain.

IV. ENCRYPTION METHODS IN CLOUD COMPUTING

To achieve security and quality of data, it is very important to provide encryption and signature based scheme.

Identity Based Encryption: Identity based encryption cryptography is a third party server uses a simple identifier as an email address to generate key that can be used for encrypting and decrypting electronic data. Typical public key cryptography greatly reduces the complexity of the encryption process for users. Identity based encryption depends on the third party identity based encryption server that generates private keys, information stores permanently is a secret master key a large random number that is exclusive to the security domain. The server uses this key to create a common set of public key parameters that are given to each user, the persons who are installed the identity based encryption software setup. When an outsourcing sender creates an encrypted message the identity based software on his system uses three parameters to generate the public key for the message.

Linear Search Algorithm: A symmetric encryption algorithm is used to encrypt the plain text for the cipher text of each keyword under symmetric encryption scheme a pseudo random sequence is generated with a length less that of the cipher text. At the same time check sequence is generated based on the pseudo random sequence and the cipher text. The sum of the lengths of the pseudo random sequence and the check sequence equals the length of the cipher text, the sum of the lengths pseudo random sequence equals the length of the cipher text.

© 2013, IJCSMC All Rights Reserved

Identity Based Signature: identity based signature scheme is deterministic if the signature on a data by the same user is same, setup generates a private key provides the security parameter as the input to this algorithm generates the systems parameters and master private key. User extract his identity to private key generates as input and obtains the private key D and send to user through a secure channel. For generating a signature on a message m the users provides his identity private key D parameters and the message as input, the algorithm generates a valid signature on message by the user.

Attribute Based Encryption: The attribute and policies associated with the message and the user decides which user can decrypt a cipher text; the authority will create secret keys for the users based on attribute for each user. Users in the system have attributes receives a key from an authority for its set of attributes. Cipher text contains a policy predicate over the attribute space.

Homomorphic Encryption: Homomorphic encryption is cryptography which promises to make cloud computing perfectly secure a web user would send encrypted data to a server in the cloud, without decrypting it and send back a still encrypted result data. Sometimes however the server needs to know something about the data its handling otherwise some computational tasks become prohibitively time consuming if not outright impossible. Suppose for instance the task we outsourced to the cloud is to search a huge encrypted database for the handful of records that match an encrypted search tem. Homomorphic encryption ensures that the server has no idea what the search term or which records matches it. As a consequence however it has no choice record in the database. The user's computer can decrypt that information to see which records matched and which did not match then assuming much of the computational burden that was trying to offload to the cloud in the first.

V. RISK IN CLOUD COMPUTING

5.1. Risk in Cloud Computing: many concern in cloud computing which cannot be well protected by traditional security approaches. Cryptography is best practice for securing data at rest at the cloud provider. Fortunately hard drive manufacturers are now shipping self-encrypting drives build encryption. Encryption should also be used for data in transit authentication and integrity protection ensures that data only goes where the customer needs. Cloud providers has strong that address legal issues each customer must have its legal experts inspect cloud provider policies ensure their adequacy.

5.2. Comparative Study: Compare to previous analysis hierarchical model have multiple owners who may encrypt according to their own ways, each user obtain keys from every owner whose records wants to read would limit the accessibility are not always online process. Alternative is to employ a central authority to do the key management on behalf of all record but require to trust on a single authority may cause problems. Comparing above analysis our work shows secure sharing of hierarchical attribute based encryption stored on semi-trusted servers and focus on addressing the complicated and challenging key management issue. Achieves scalability due to its hierarchical structure but also inherits flexibility and fine grained access control in supporting compound attributes of multiple value assignments for access expiration time to deal with user revocation more efficiently than existing scheme. Using attribute based encryption policies are expressed based on the attributes of users or data which enables patient to selectively share records among a set of users by encrypting the file under a set of attributes without the need to know a complete list of users.

VI. CONCLUSION

Encryption scheme describes the amount of time and computational resource required for the evaluation. Analysis shows the attribute set-based encrypted data stores on cloud and protects from the unauthorization users mainly usefully for banking services. To prevent server from learning the file content of each segment searched by monitoring the users search patterns. Future direction of our analysis is to avoid the intrusion objects without user presence.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.
[2] M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/ 12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.
[3] H.Erdogmous, 2009. "Cloud Computing: Does nirvana hide behindthe Nebula?" IEEE Software, vol 26.
[4] D.Boneh, 2008. "Generalization Identity based and broadcast encryption achemes". Vol 5350.

© 2013, IJCSMC All Rights Reserved

[5] Richard Chow, Phillepe Goel. "Controlling data in the cloud"
[6] http://ijcttjournal.org/volume-1/issue-2/ijcctjournal-v1i2p27.pdf
[7] http://eprint.iacr.org/2011/010.pdf
[8] http://crypto.stanford.edu/ibe/

Authors Profile

P. Sravanthi pursuing M.Tech Computer Science Engineering from Vijay Rural Engineering College B.Tech Computer Science Engineering from Srinivas Reddy Engineering College. Her interested subjects include Operating system, Networking, Unified Modelling Languages, Databases & Cloud Computing.

N. Uday Bhaskar pursuing M.Tech Computer Science Engineering from Sri Indu College of Engineering & Technology. His interested subjects include Operating system, Networking, Unified Modelling Languages, Databases & Cloud Computing.

P. Swapna B.Tech Computers from Vijay Rural Engineering College M.Tech Computer Science from Kshathriya College of Engineering. She is currently Associate Professor Computer Science Department at Vijay Rural Engineering College and has guided many UG & PG students. Her interested subjects include Databases, Automata and Compiler, Web Technologies, Information Retrieval System and Mobile Computing.

Nagaraju Master of Computer Application from Holy Faith P.G.College M.Tech Computer Science Engineering from Sri Indu College of Engineering. Currently he working as Assistant Professor at Sri Indu College of Engineering & Technology interested subjects include Advanced Data Structures Java Object oriented Programming.

© 2013, IJCSMC All Rights Reserved