A Survey on Security of Data outsourcing in Cloud

Swapna Lia Anil[1], Roshni Thanka[2]

[1]Post Graduate student, Department of Computer Science and Engineering, Karunya University, India
[2]Assistant professor, Department of Computer Science and Engineering, Karunya University, India

Abstract- Cloud computing enables on-demand access to shared resources. It lets to use files and applications over the internet. This technology uses both the internet and the central servers to maintain data and resources. Many organizations uses cloud computing services to outsource their data into cloud environment for location independent resource pooling, elasticity and usage-based pricing. Since more enterprises store their private data on the cloud storage, privacy and security become major concern. One of the most challenging problem in Cloud computing is about the security of the outsourced data which is mainly handled by untrusted parties. This paper surveyed different types of techniques used to enhance the security of data stored in cloud environment and compare those techniques.

Index Terms- Cloud computing, Data outsourcing, Data access control, Privacy, Security.

I. INTRODUCTION

Cloud computing relies on sharing computing resources rather than having local servers to handle applications for a particular organization or individuals. Since there is no infrastructure investment needs, the expand or shrink resources based on demand, payment based on usage makes it popular among various technologies. Many enterprises look for these benefits to be utilized to maximum extend. Cloud service makes it possible to access information from anywhere at any time. Cloud computing uses networks of large groups of servers typically low-rate consumer PC technology, spread data processing with specialized connections.

The virtualization techniques maximize the power of cloud computing. Using this concept, cloud computing can also supports heterogeneous resources and flexibility is achieved. The flexibility of cloud computing is a function of allocation of resources on demand. Cloud computing also allows immediate scaling. Cloud computing is a comprehensive solution that delivers IT as a service. It is an internet based solution for computing resources. Data stored in cloud storage is considered as data outsourcing. This data is managed by cloud service providers which is an external party. Cloud services provide a cost effective management of resources, more and more enterprises utilizes this benefit. Since cloud storage is managed by external parties, they cannot be trusted fully. Here security and privacy becomes a major concern.

The cloud security involves restricting access to authorized users, maintaining the integrity of data and ensuring the availability of data and services. Mainly the security includes confidentiality, integrity and availability. By moving storage, applications, other IT infrastructure and services to the cloud, results in increased reliability and flexibility, with low costs but the information security is a major problem. For the security of outsourced data generally the data is stored in encrypted form so that only authorized users can access data.

The objective of this paper is to focus mainly on various cryptographic key management for security. The remaining portion of the paper is organized like this. Section II presents the key concepts of this paper. Section III presents existing workflow scheduling algorithms and section IV concludes the paper with summary.

II. KEY CONCEPTS

The main concepts dealing in this paper are cloud computing and cryptographic key management for security. Cloud computing is a technology that delivers on demand access to shared resources over the internet. With the storage of data in cloud a customer can reduce their burden to maintain the infrastructure for housing the data. But this cannot ensure the security of data in the cloud environment. The data stored in a cloud should be secure enough so that more enterprise can rely on this technology. Confidentiality and privacy are the most important factors related to security. Any organization can depend on cloud service providers in order to keep their data, thereby reduce the cost. If a cloud provider can provide maximum security to the data of their customers, they can catch the attention of more people. Even the customer should also have some control over the security of their data stored in the cloud environment. The major issue concerned with the data stored in the cloud is the security of the data. If the outsourced data in the cloud environment is managed by multiple outsources having different access rights then the security of the data stored in cloud storage become more challenging.

A. Cloud computing

A cloud makes it possible to access information from anywhere in the world at any time provided internet connection should be available. It is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and represented as one or more unified computing resources based on service level agreements established through negotiation between the service providers and consumers. There are different types of cloud depending on needs. This includes private cloud, public cloud, community cloud and hybrid cloud. Public cloud can be accessed using internet connection by any subscriber. Google and Microsoft provide public cloud. A private cloud is build for specific group or oraganisation with access limited to that group. Community cloud is shared among organization with similar cloud requirements. Hybrid cloud is a combination of atleast any of two cloud type.

According to the type of services provided cloud computing is classified into three: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS). These are

the service models. IaaS Clouds, example Amazon, provide virtualized hardware and storage where the users can deploy their own applications and services. PaaS Clouds, like Microsoft Azure, provides an application development environment for users which help them to implement and run applications on the Cloud. According SaaS cloud there are two types of Cloud, which delivers software applications to the users. The first group offers the entire application as a service to the end users, which is used without any changes or customization. Examples of these types of clouds are Google office automation service, like Google Document or Google Calendar. The second group provides on-demand web services to the users, which can be used to build more complex applications.

B. Security in cloud

The information stored in the cloud owns by some other person or organization other than the cloud owner. The data stored in the cloud may be valuable, so it should be secure enough so that no one could have access to these data other than the authorized person. The data stored in a cloud environment is handled by external parties so it can be called as outsourced data. The data are stored in such a way so as to make it independent of geographic location, to reduce the cost to maintain the requirements for storage like hardware and software. The main advantage over the cloud is the usage based pricing and the ready availability of the resources without even care about its maintenance. But since everything have its own pros and cons, cloud too have some cons. The main difficulty is with the security and privacy of the data stored on the cloud environment. The data in a cloud are handled by untrusted parties which may result in insecurity of data. In order to solve this problem one have to take measures to make the data secure. There exist many security measures for the data stored on cloud.

III. EXISTING SECURITY MEASURE FOR DATA STORAGE IN CLOUD

The following are some of the techniques that are currently present in clouds and are summarized .

1. A robust single server solution for remote querying of encrypted database on untrusted servers is presented by Damini E [1, 2]. It uses indexing approach. Here indexing information will be attached with encrypted database, which is used by server to select data to be returned in response to a query without revealing the contents in database. The indexes balance the trade-off between query execution efficiency requirements and protection requirements due to inference attack exploiting indexing information. It also investigates quantitative measures to model inference exposure.
2. Atallah MJ [4, 5] proposed a solution to the key management hierarchies by the following properties: space complexity of public information is same as storing the hierarchy; the private information in a class have single key associated with that class; updates are handled locally in hierarchy; the scheme is strong against collusion; each node derive key of descendant. In addition provided a technique for reducing distance between nodes for faster key derivation.
3. Two layer of encryption imposed on data is another approach to protect the data. The owner imposes the inner layer for initial protection. The server imposes the outer layer for policy modifications. This two layer protection provides efficient and robust solution. Thus an approach for policy evolution takes into account the main feature and guarantee confidentiality of information in the presence of significant policy updates, identifies the exposure to collusion when risk arise. Di Vimercati [6, 7] presented this technique for the data security.
4. Wallner [8] proposed another approach which focuses on two main areas of concern with respect to key management: initializing multicast group with common net key and rekeying the multicast group. The important feature regarding multicast key management is to identify a technique. This technique allows for secure compromise recovery, and it is robust against collusion of excluded users. This technique maximizes the number of transmissions required to rekey the multicast group and imposes minimal storage requirements on the multicast group.
5. A novel solution to scalability problem of group/multicast key management is proposed by Wong [9]. Here secure group is formalized as a triple (U, K, R) where U indicates a set of users, K denotes set of keys held by the users, and R is the user-key relation. Then introduce key graphs to specify secure groups. A special class of key graphs, present three strategies for securely distributing rekeys messages after a join/leave, and specifies protocols for joining and leaving as a secure group. These are implemented in a prototype group key server built and it presents measurement results from experiments, thereby shows group key management.

Table 1 Existing approaches comparison

Approach	Merits	DeMerits
Dynamic and efficient key management for access hierarchies.	Updates are handled locally A single key associated with a node.	With parent node key, child would be known.
Balancing confidentiality and efficiency in untrusted relational DBMSS.	Indexing for easy access.	Extra space required for index table.
Efficient key management for enforcing access control in	Key derivation graph. Minimizes the total number of keys.	Maintain graph Problem.

outsourced scenarios.		
A data outsourcing architecture combining cryptography and access control.	Combination of access control and cryptography	Over encryption
Preserving confidentiality of security policies in data outsourcing.	Privacy of the tokens published in the public catalogue.	Encryption layer to the catalog required.
Secure integration of asymmetric and symmetric encryption schemes.	Uses both asymmetric and symmetric properties.	Complex calculation involved
Simple and fault-tolerant key agreement for dynamic collaborative groups.	A novel approach to group key agreement	With parent node key, child would be known.
Scalable hierarchical access control in secure group communications.	Reduces the communication, computation and storage. Overhead associated with key management	With parent node key, child would be known.
Secure and efficient access to outsourced data.	Fine grained access control to outsourced data. Flexible and efficient key management.	Unauthorized users can access to child node once parent node is known.
Secure group communications sing key graphs.	Key graphs to specify secure groups.	Storage overhead.
Reliable group rekeying: a performance analysis.	Improved scalability.	With parent node key, child would be known.

IV. CONCLUSION

Security of data in cloud is one of the major issue in cloud computing environment. This paper surveyed the various existing security measures in cloud computing and compare their various security parameters. To provide security of data in cloud is one of the major issue, which hold back the clients to store their data in cloud environment. Even though the security problems cannot be solved completely, better and powerful security measures can be applied to provide maximum security which can gain the trust of clients to store and access their data from the cloud storage.

REFERENCES

[1] Damini E, Di Vermercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P, 2005, ‘‘Key management for multi-user encrypted databases’’, *In:Proceedings of the 2005 ACM workshop on storage security and survivability*.pp.74-83.

[2] Damini E, Di Vermercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P, 2007, ‘‘An experimental evaluation of multi-key strategies for data outsourcing”, *In:New approaches for security, privacy and trust in complex environments,IFIP international federation for information processing*,pp.385-96.

[3] Damini E, Di Vermercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P, 2003, ‘‘Balancing confidentiality and efficiency in untrusted relational DBMSS’’, *SIGMOD RIn:Proceedings of the 10th ACM conference on computer and communications security*,pp. 93-102.

[4] Atallah MJ, Frikken KB, Blanton M, 2005 “Dynamic and efficient key management for access hierarchies” *In:Proceedings of the 12th ACM conference on computer and communications security*, pp. 190–202.

[5] Atallah M J, Blanton M, Fazio N, 2009, Frikken KB, “Dynamic and efficient key management for access hierarchies” *ACM Transactions on Information and System Security*, pp.18:1–43.

[6] Di Vimercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P, 2006, “Over-encryption: management of access control evolution on outsourced data”, *In:Proceedings of the 33rd international conference on very large databases*, pp.123–34.

[7] Di Vimercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P, 2007, “A data outsourcing architecture combining cryptography and access control” *In:Proceedings of the 2007 ACM workshop on computer security architecture*, pp.63–9.

[8] Wallner D, Harder E.Agee, 1999, “Rfc2627:key management for multicast:issues and architectures”, pp56.

[9] Wong CK, Gouda M, Lam SS, 1998, “Secure group communications sing key graphs”In: Proceedings of theACM SIGCOMM’98 conference on applications, technologies, architectures, and protocols for computer communication, pp.68–79.