Efficient Cloud Storage Confidentiality to Ensure Data Security

Dr. L. Arockiam
Associate Professor,
St. Joseph's College, Trichy,
Tamilnadu, India
larockiam@yahoo.co.in

S. Monikandan
Research Scholar,
M S University, Tirunelveli
Tamilnadu, India
moni.tamil@gmail.com

Abstract – **Cloud computing provides an enormous amount of virtual storage to the users. Cloud storage mainly helps to small and medium scale industries to reduce their investments and maintenance of storage servers. Cloud storage is efficient for data storage. Users' data are sent to the cloud is to be stored in the public cloud environment. Data stored in the cloud storage might mingle with other users' data. This will lead to the data protection issue in cloud storage. If the confidentiality of cloud data is broken, then it will cause loss of data to the industry. Security of cloud storage is ensured through confidentiality parameter. To ensure the confidentiality, the most common used technique is encryption. But encryption alone doesn't give maximum protection to the data in the cloud storage. To have efficient cloud storage confidentiality, this paper uses encryption and obfuscation as two different techniques to protect the data in the cloud storage. Encryption is the process of converting the readable text into unreadable form using an algorithm and a key. Obfuscation is same like encryption. Obfuscation is a process which disguises illegal users by implementing a particular mathematical function or using programming techniques. Based on the type of data, encryption and obfuscation can be applied. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.**

Keywords: - Cloud Storage; Data Protection; Confidentiality; Encryption; Obfuscation;

I. INTRODUCTION

Cloud computing delivers massively scalable computing resources as a service with Internet based technologies. Resources are shared among a vast number of consumers allowing for a lower cost of IT ownership [1]. At present, cloud computing is widely discussed in academia and industry. Virtualization, distributed computing technology and so on, cloud computing integrates the computing, storage, networking and other computing resources, and then leases to users. Such mode could reduce the cost of enterprise information construction and accelerate the informatisation of enterprise. The Cloud storage is designed for virtualized computer environment. The cloud storage is implemented using cloud computing that means utilizing the software and hardware resources of the cloud computing service provider. Cloud computing is growing at a very high velocity in the IT industry around the world. While there are many advantages of cloud computing, the enterprises are still waiting to use cloud computing, because of the data security problem of cloud computing is not solved completely. Cloud Storage provides a virtual space to store bulk data. But the data owners have no control over their data. The cloud provider has full control on the user's data. This makes the user's mind to thing about the data security in the cloud.

Data protection in the cloud storage is the core security problems. Data protection [2] is concerned with data confidentiality, integrity, authentication, availability and so on. Data confidentiality means that only authorized persons can use the data. Data integrity refers to information that has not been modified or remains untouched. Authentication refers to the process of verifying whether the incoming user is authorized or not. Data availability refers to the ability to guarantee to use data in time when needed and also refers to the availability of cloud service provider on-demand.

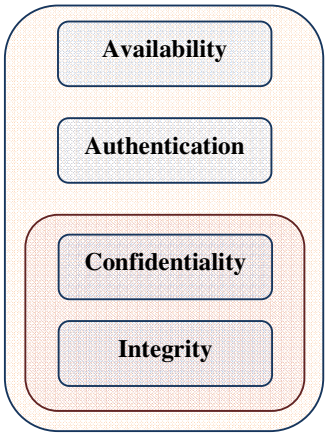

Fig.1 Layers of Data Security

Fig.1 represents the layers of data security in the cloud. First layer is availability, which ensures the availability of cloud computing resources or availability of the cloud providers needed when on-demand. Second layer is authentication, which helps to protect the unauthorized user's entry to the cloud. Third layer is confidentiality, which ensures

[978-1-4799-2352-6/14/$31.00 ©2014 IEEE]

only the data can be accessed by the privileged cloud users. Last layer is integrity, which ensures that cloud data could not be modified by unauthorized cloud users. Authentication technique can be used to protect the data from outsiders attack. Confidentiality could be used to protect the data from outsiders as well as insiders attack. If the confidentiality of the data is ensured completely, then integrity will also be ensured. If the data in cloud storage can't be accessed by the intruders then it cannot be modified or altered by intruders. Even though the authentication mechanism is broken by the attackers, the data in the cloud is still be secured when an efficient confidentiality mechanism is used.

This paper proposes an efficient cloud storage confidentiality technique by using encryption and obfuscation technique [3]. Normally, confidentiality is ensured by encryption technique, but for the cloud environment encryption alone is not enough for data protection. Encryption is integrated with obfuscation technique. Obfuscation technique alone is also not enough to adopt for complete confidentiality of data in cloud storage because the user can find values through reverse engineering or by using brute force technique, which may compromise cloud data security. This paper uses encryption and obfuscation techniques in an integrated manner to protect the data from the attackers (insiders and outsiders). In the proposed technique, users should encrypt and obfuscate the data whatever they want to send to the cloud storage. Encryption and obfuscation could be done from user's side.

II. DATABASE MANAGEMENT IN THE CLOUD

Outsourcing of database management [4] is a necessary component of cloud computing. Due to the rapid advancements in network technology, the cost of transmitting a terabyte of data over long distances has decreased significantly in the past decade. In addition, the total cost of data management is five to ten times higher than the initial acquisition cost. This will lead the industries to outsource their data with cloud storage provider with minimum rate [5]. Database outsourcing model will enable the cloud users for better utilization of their data.

A Cloud database management system (CDBMS) [6] is a distributed database. It delivers computing resources as a service instead of a product. Cloud database outsourcing system is a sharing virtual storage spaces. It can be accessed by the internet. Cloud delivers several services, like, Software as a Service or SaaS, which is an application that is delivered through the browser to customers. Cloud applications connect to a database that is being run on the cloud. Some cloud databases are manually configured; some are preconfigured, and some are native. Native cloud databases are conventionally outfitted and steady that is modified to adapt to the cloud.

Despite the advantages offered by cloud-based DBMS, many people still have apprehensions about them. This is most likely due to the various security issues that have yet to be dealt with. These security issues stem from the fact that cloud DBMS are hard to monitor since they often span across multiple hardware stacks and/or servers. Security becomes a serious problem with cloud DBMS when there are many Virtual Machines (which might be accessing databases via any number of applications) that might be able to access the database without being noticed or setting off any alerts. In this type of situation, a malicious person could potentially obtain pertinent data or cause serious harm to the integral structure of the database, putting the entire system in risk. This is the main problem with the cloud data storage. Thus, an efficient security model needs to address this issue in the cloud data storage.

III. RELATED WORK

Ensuring confidentiality of user's data in cloud storage is the main research problem around the cloud computing. Cloud storage providers store users critical data; it needs to be secured. Cloud computing has a recent success in information technology and will dominate the IT industries in the coming years. Cloud computing also faces the overwhelming challenges. To ensure the proper physical, logical and personnel security controls, especially in cloud data storage are more significant. Moreover, while moving such large volumes of data, the management of the data may not be fully trustworthy. This section describes the research works which are related to ensure the confidentiality of data in cloud storage.

Dr. Nashaat el-Khameesy and Hossam Abdel Rahman in [7] proposed a security policy and procedures explicit to enhance the Data storage security in the cloud. They had a Control Access Data Storage (CADS) that included the necessary policies, processes and control activities for the delivery of each of the Data service offerings. The collective control Data Storage encompasses the users, processes, and technology needed to maintain an environment that supports the effectiveness of specific controls and the control frameworks. The security, correctness and availability of the data files being stored on the distributed cloud servers. It must be guaranteed by Providing Security Policy and Procedure for Data Storage, Defense in Depth for Data Storage in the cloud, Correctness Verification and Error Localization computing. All this recommendations are only theoretically proposed.

R. Anitha et al. of [8] proposed a method for providing protection to the data stored at the data server through metadata. This process provides protection using a cipher key which is created from the features of metadata. In this model, the time required for generating the cipher key is proportional to the number of attributes in the metadata as well the algorithms used for cipher key generation. Their plan enforced safety by providing two novel features; 1. Security is provided by the proposed design, where the encryption and decryption keys cannot be compromised without the involvement of data owner and the metadata data server (MDS). 2. The cipher key generated using the modified feistel network holds good for the avalanche effect as each round of the feistel function

depends on the previous round value. This approach is time consuming for generation cipher key.

B. Raja Sekhar et al. of [9] introduced the Ciphertext policy attribute-based encryption (CP-ABE) which is a promising cryptographic solution to ensure the data security and integrity in cloud storage. It allows data owners to define their own access policies over user characteristics and enforce the policies on the data to be distributed. It provides a way of defining access policies based on various characteristics of the requester, background, or the data object. Especially, ciphertext-policy attribute based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt several pieces of data per the security policy.

To ensure the correctness of users' data in the cloud, Cong Wang et al. [10] proposed a distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, they also achieve the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike the most prior works, the new plan further supports secure and efficient dynamic operations on data blocks, including data update, delete and append.

IV. Cloud Storage Issues

There are several types of issues [11] that cloud storage users both at enterprise level and as an individual consumer might face during the use of the service. Most of the issues are with security of the data in the cloud. Ensuring this problem in the cloud storage is most significant for the cloud usage businesses. The data is confidential and available when it is needed. Let us look at these facts in a more detailed manner. This is not an exhaustive list but certainly covers some of the more urgent and vital matters.

A. Trust.

Data, when stored in the cloud, needs not only to be confidential but also should be accurate every time it retrieved after uploaded or a modification. There should not be a loss of integrity of the data. This is a valid scenario when third party storage services are compromised by the malicious agents. The data that is being provided by the corrupted service might not be accurate or fresh. This can be sometimes very hard to detect and can sometimes lead to considerable information leakage before being discovered. Hence a set amount of duty to the cloud service user to trust the cloud provider that what they provide is accurate inside the boundary of integrity check. The guidelines have been agreed upon between the service provider and the user. The guidelines might not be correct when the service provider's infrastructure has been compromised or encountered an error [12].

B. Cloud Service provider agreements.

Use of the cloud storage service will become more of a commodity market, security would be needed and be necessary to differentiate service providers and systems. This is not the case right now in the industry since most of the cloud service providers today provide service level agreements with emphasis on high data availability with little guarantee on the protection of the data. [13] Due to internal errors or sometimes malicious changes to their system the data might be exposed or given to the users of the system with the integrity being compromised. This trend does not help the customers using the service to prove that their data has been compromised if and when this happens.

C. Data history.

One of the significant features with local data storage is the presence of metadata features which allow users to view the history of a data object. This allows the systems to provide data integrity checks and rollback capabilities when a corruption or compromise is detected in the system. These features are almost non prevalent in the existing cloud system, and if present there are substantial security vulnerabilities associated with it because of the scale of the service. This feature has become de facto for ordinary storage system on local systems. It provided by most of the data storage systems needs to be implemented in the cloud service.

D. Data Possession.

This problem is loosely related to one of the other issues looked into how to trust the data stored on the service provider. When data is retrieved from the service provider on performing an integrity check, it would be very hard to determine how the data was stored in the service providers system. This is to ensure that the data is not leaked to a third party to whom the service provider is outsourcing the data, when the agreement for service is being agreed upon by the service provider and customer. The present service providers give hardly any kind of security on where and how the data is being stored and how secure is the methods.

V. Proposed Confidentially Technique

Cloud computing provides an efficient storage setting to store and retrieve the cloud users critical data. Ensuring data security is a vital role to cloud users as well as cloud providers. This paper uses the confidentiality parameter to address the data security problems. Fig.2 represents the cloud storage confidentiality protection system using encryption and obfuscation technique. All the data must be encrypted or obfuscated before it is sent to the cloud database. Based on the type of the data, encryption or obfuscation can be used. Once the data is applied by proposed confidentiality technique, then the data is submitted to the cloud storage. Encryption and obfuscation of cloud data is done in the user side. The key used for encryption algorithm is generated in the user environment.

Generally, Confidentiality is ensured by encryption algorithm. For cloud data storage, Symmetric encryption is

best choice, because symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [14]. Along with the encryption algorithm [15], this paper also uses the obfuscation technique to improve the data confidentiality in cloud storage.

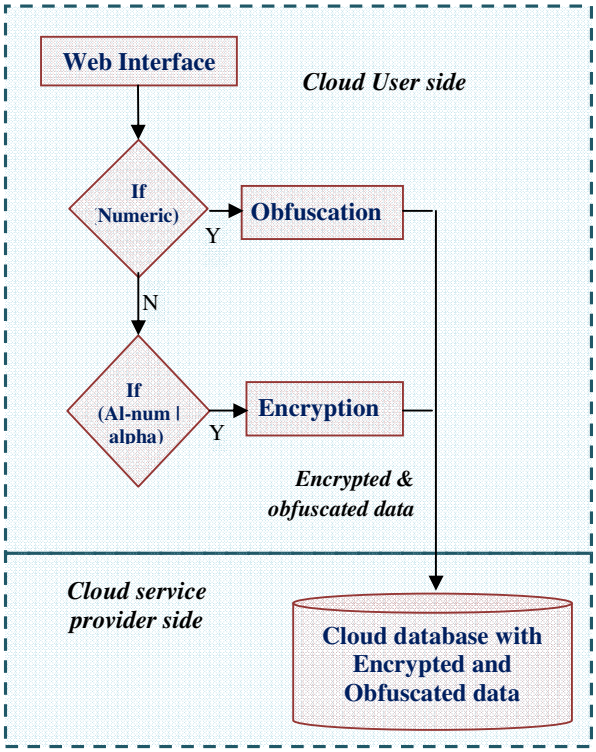

Fig. 2 Proposed Technique for cloud storage confidentiality using Encryption and obfuscation

Algorithm#1 is used to find out the type of data (T) which is ready to store in the cloud storage. Based on the type of data, encryption or obfuscation is applied on the data before forwarded to the cloud. If the data (T) are digits, then obfuscation technique is applied, if the data are alphabets or alphanumeric then encryption is applied on the data. This algorithm will call the corresponding algorithm based on the data type of (T).

Algorithm #1

1. *start*
2. *T=plaintext*
3. *if (T equal to isdigits()) then*
   obfuscation_digits(T)
4. *end if*
5. *if (T equal to isalphanum()) then*
   encryption_text(T)
6. *end if*
7. *if (T equal to isalpha()) then*
   encryption_text(T)
8. *end if*
9. *end*

Algorithm#2 is used for obfuscation. This algorithm is used for numeric data type. Obfuscation is a technique by applying through specific mathematical functions or by using programming techniques. This algorithm doesn't use any key to mask the user's data. There is no. of obfuscation related techniques are available. This paper uses two mathematical function namely root() and floor() functions. These two mathematical functions applied to the data to obfuscate them.

Algorithm #2

1. *obfuscation_digits(T)*
2. *start*
3. *for i=1 to size of(T) then*
4. *d=root(T)*
5. *C=floor(d)*
6. *loop*
7. *end*

Algorithm#3 is used for encryption. This algorithm is used for numeric or alphanumeric data type. This is a symmetric encryption algorithm. The algorithm uses substitution and transposition technique to convert the plain text into cipher text. ASCII codes of the plain text are used throughout the algorithm. It uses four keys for encryption, and same keys are used for decryption also.

Algorithm #3

1. *encryption_text(T)*
2. *start*
3. *Convert (T) into ASCII code*
4. *N= count (T)*
   // N-no.of character in T excluding whitespace
5. *Form a square matrix MAT [MxM] > N*
   // M-order of matrix
6. *Apply (T) into the matrix from left to right*
7. *Divide the Matrix MAT into three matrix called UMAT,DMAT,LMAT*
   //UMAT-Upper Matrix
   //DMAT-Diagonal Matrix
   //LMAT-Lower Matrix
8. *Read the Text T by UMAT(U), DMAT(D) and LMAT(L)matrix*
   //U, D, L- text of upper, diagonal and lower matrix respectively
9. *Generate three keys (K_1, K_2, K_3) for each matrix.*
10. *Apply the key K_1, K_2, K_3 for U, D, L*
    // [U-K_1, D-K_2, L-K_3]
11. *Apply the resultant text (from step 10) into another matrixMAT_1 [MxM]*
12. *Generate another key called K_4*
13. *Order the matrix based on the key K_4*
14. *Read the matrix by column using the order of key K_4*
15. *Resultant text from step 14 is converted from the ASCII code into character(C)*

//C-Cipher Text
16. end

Proposed cryptography technique uses encryption and obfuscation for the different type of data. Integration of obfuscation technique with encryption technique has given more confidentiality than they used in separately. Confidentiality of cloud data is ensured by using this technique. This can protect the data in cloud storage from insiders as well as outsiders attack.

To simple understanding of the proposed cryptography technique, consider a sample transactional table as shown below Table I, to be stored in the cloud storage. This Table I values are applied by the proposed cryptography technique.

TABLE I. TRANSACTIONAL TABLE WITH PLAIN TEXT

Trans_Id	Cust_Id	Item_Name	Quantity	Total_P
TId_1003	A230kum	Lux	4	1020
TId_923	B301sus	Himalaya	7	605.25
TId_2304	C100mon	Bovonto	3	145
TId_9087	B002lav	Laxmi	5	100
TId_0012	G123aro	Medicine	12	1600
TId_9999	X987ren	Chocolate	8	450

Based on the proposed technique, encryption and obfuscation can be applied on the Table I. Alphabets and alphanumeric types of data are encrypted, and numeric types of data are obfuscated. The Table II shows the cipher text value of Table I.

TABLE II. TRANSACTIONAL TABLE WITH CIPHER TEXT

]zUdbju|p	L!pvL|xh"	RymhQnwhy	Zz!dljx}&	]m\wb}ru{
]k<g3mL:?	J<y6x<5t>	U,{{k"x\l	16	32
]k?g5mLBU	K= 3x96l?	Qm&pdvlum	49	25
]k<g6mL;@	L<z3r94v=	K{{yw rw{	9	12
]kDg3mLBC	K>#3d93u<	Uy%{drdry	25	10
]k=g3mL9>	P?{5u;4j=	Vuzglmhlq	144	40
]kEg<mLBE	aCz;hA<{E	Lomronkx!	64	21

User's data like the transactional table Table I is submitted to the cloud storage in the form of encrypted and obfuscated shown in Table II. This will increase the data security in the cloud storage.

VI. CONCLUSION

Cloud computing is profitable computing services to an individual and enterprise customers. But due to some of security problem in it, people might be reluctant use it. Once the issues are resolved, cloud computing will be the trillion dollars business in the computing world. The Data storage on un-trusted cloud makes data security as a challenging problem. Data security in the cloud is ensured by the confidentiality of sensitive data should be enforced on Cloud storage service providers. This paper proposed a new cryptographic technique which is applied to address this problem. Encrypted data are stored on storage servers while secret key(s) are retained by data owner; access to the user is granted by issuing the corresponding data decryption keys. Along with encryption, obfuscation technique is used to increase the confidentiality of data. Algorithms are proposed for encryption and obfuscation technique. The user data are encrypted or obfuscated before they are forwarded to the cloud storage. The Proposed technique is secure to store the cloud users' data in the cloud storage. Encryption only or obfuscation only is not sufficient for cloud data storage. Integration of both techniques should provide maximum security to user's data in the cloud data.

REFERENCE

[1] Uegebe Ikechukwu Valentine and Omenka Ugochukwu Enyinna, " Building Trust and Confidentiality in Cloud computing Distributed Data Storage", West African Journal of Industrial & Academic Research, Vol. 6 No.1 March 2013, pp78-83.

[2] Xiaojun Yu, Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle", International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, Dec 2010, pp 1-4.

[3] Atiq ur Rehman, M.Hussain, "Efficient Cloud Data Confidentiality for DaaS", International Journal of Advanced Science and Technology Vol. 35, October 2011, pp 1-10.

[4] Masayuki Okuhara et al, "Security Architecture for Cloud Computing", FUJITSU Sci. Tech. J., Vol. 46, No. 4, October 2010, pp. 397-402.

[5] Yvette E. Gelogo and Sunguk Lee, " Database Management System as a Cloud Service, International Journal of Future Generation Communication and Networking Vol. 5, No. 2, June 2012, pp 71-76.

[6] Hyun-Suk Yu, Yvette E. Gelogo, Kyung Jung Kim, "Securing Data Storage in Cloud Computing", Security Engineering Research Institute (Journal of Security Engineering), No. 9, No. 3, June 2012, pp 251-260.

[7] Nashaat el-Khameesy, Hossam Abdel Rahman, " A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems", Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, June 2012, pp 970-974.

[8] R. Anitha, P. Pradeepan, P. Yogesh, and Saswati Mukherjee, "Data Storage Security in Cloud using Metadata", 2nd International Conference on Machine Learning and Computer Science(IMLCS'2013), Kuala Lumpur (Malaysia), August 2013, pp 26-30.

[9] B. Raja Sekhar, B. Sunil Kumar, L. Swathi Reddy, and V. Poorna Chandar "CP-ABE Based Encryption for Secured Cloud Storage Access", International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012, pp 1-5.

[10] Cong Wang,Qian Wang,Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International Workshop on Quality of Service, IEEE, IWQoS, July 2009, pp 1-9.

[11] Anup Mathew, "Survey Paper on Security & Privacy Issues in Cloud Storage Systems", EECE, Term Survey Paper, April 2012, pp 1-13.

[12] Prince Mahajan, Srinath Setty, Sangmin Lee, Allen Clement, Lorenzo Alvisi, Mike Dahlin, and Michael Walfish, "Depot: Cloud storage with minimal trust", 9th USENIX Symposium on Operating System Design and Implementation, 2010, pp 1-26.

[13] Raluca Ada Popa, Jacob R. Lorch, David Molnar, Helen J. Wang, and Li Zhuang, "Enabling Security in Cloud Storage SLAs with CloudProof", USENIX Annual Technical Conference, 2011, pp 1-12.

[14] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", O'Reilly Media, Inc., chapter 4, September 2009, pp 61-71.

[15] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2013, pp 3064-3070.

[16] S Kamara, K Lauter, "Cryptographic Cloud Storage", IFCA/ LNCS 6054, Springer-verlag, Berlin Heidelberg, 2010, pp 136-149.