A Multi-Level Security Mechanism for Cloud Storage System

Syed Tasleem[1], P. Vijayaraghavulu[2]
[1]PG Student, Dept of CSE, Sri Annamacharya Institute of Technology and Science, Rajampet, Kadapa
[2]Asst.Professor, Dept of CSE, Sri Annamacharya Institute of Technology and Science, Rajampet

***Abstract* - Cloud computing is a highly scalable distributing computing platform in which resources are offered as services. The security of data in cloud is one of the important issues which act as an obstacle in the implementation of cloud computing. This paper is proposing an efficient cloud security model in which the model is providing the multi-level encryption mechanism over the data to be uploaded at the cloud as well as role-based authentication for the users. The model is including four parties: Data owner, Private Cloud, Admin and User. The encryption mechanism is using the RSA algorithm first and further re-encrypts the data with MD5 to enhance the security of the data. The Message authentication Code is being generated before uploading the encrypted data which will be used after downloading of the data. The Message Authentication Code of downloaded data will be decrypted first by user and then send to Data owner for data integrity check. After that the user can decrypt the downloaded data if he gets confirmation from Data owner. The model is using the best possible multiple techniques in a single approach.**

***Index Terms* - Cloud Computing, Encryption, Message Authentication Code, Role-based Authentication.**

1.INTRODUCTION

Cloud computing has been visualized as the next generation of distributed computing in an emerging network field. The National Institute of Standards and Technology (NIST) describes emerging cloud environment by four deployment models, five essential characteristics and three service models. The three models are infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS). Some of the features of cloud computing are broad network access, location-independent resource pooling, rapid resource elasticity, on-demand self-service, and measured service. The three service models in cloud are private cloud, public cloud, community cloud, and hybrid cloud. In this paper adaptive multilevel security framework based on data sensitivity that manages to provide adequate level of security for the data classified under different classes. The essential characteristics of cloud computing are on demand self-service, broad network access, measured service, rapid elasticity, resource pooling and so on.

The data stored in cloud environment can be accessed from anywhere and at any time and by anyone. Many techniques effectively provide the security for cloud storage data. During transmission of data in cloud environment, encryption is an efficient and widely used technique for data security. It can be done by public key, private and other identical information between the sender and receiver. Cloud storage is a place where we store huge volume of data and it can be accessed from anywhere and by anyone and in anytime. The main advantage of cloud storage is there is need not to pay for the storage of data. Despite of the cloud storage advantages; outsourcing data storage may threaten the sensitive data of users. Because in cloud environment the data are distribute in various locations. It may lead to unauthorized physical access to the data. So, it is necessary to secure the data in cloud environment. Encryption is the most effective technique to transmit the sensitive data in cloud environment. There are various techniques and mechanism was developed to provide security for cloud storage data.

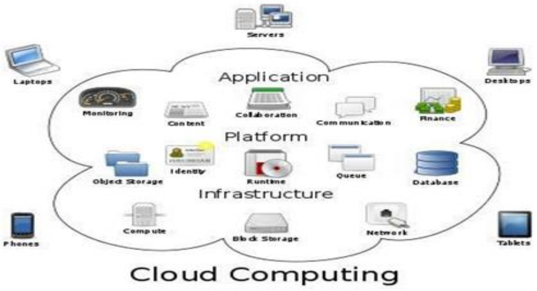


Fig-1 Cloud computing framework

Provides security based on data sensitivity. The data needs to be secured throughout the progress, security of the data in cloud is a major challenge to be concentrated on because the data is in third party's premises.

This paper suggests an adaptive multilevel security framework based on cryptography techniques that provide adequate security for the classified data stored in cloud. Proposed Multilevel of security of data with different sensitivity that changes with business needs and commercial conditions.

2 ISSUES IN CLOUD COMPUTING

Several restrictions to the widespread adoption of cloud computing remain. Some of them are explained below:

2.1) SHARING INFORMATION WITHOUT A WARRANT

Cloud providers can share information with third party auditors (TPA) if necessary, for purposes of law and order even without a warrant. Here, the owner of the data has to be permitted in their privacy policies which users have to agree to before they start using cloud services models. There is life- threatening situations in which there is no time to wait for the police to issue a warrant. Most of the cloud providers can share information immediately to the police in such situations to get warrant for the sensitive data.

2.2) SECURITY

Security is generally a desired state of being free from harm. As defined in information security, it is a condition in which an information asset is protected against its confidentiality, integrity, and availability in the desired state and at the right time. Security for the cloud is most important aspect, there are a number of issues to be addressed if the cloud is to be perfectly secure. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. Various security mechanisms are recognized as the features of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that can be shared multi-user mainframe security models apply with cloud security.

CONSUMER AND STORAGE

The various use of cloud computing could lead to a reduction in demand for high storage capacity consumer end devices, due to cheaper low storage devices. Despite of the cloud storage advantages; outsourcing data storage may threaten the sensitive data of users. It may lead to unauthorized physical access to the data. Encryption is the most effective technique to transmit the sensitive data in cloud environment. The specialized nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans.

SUSTAINABILITY

Although cloud computing is often assumed to be a form of green computing, there is currently no way to measure how "green" computers are. Environmental problem associated with the cloud storage domain is energy use. Traditionally clouds are concerned that this new explosion in electricity use could lock us into old, polluting energy sources instead of the clean energy available today." Greenpeace ranks the energy usage of the top ten big brands in cloud computing, and successfully urged several companies to switch to clean energy. The various energy efficiency in cloud computing can result from energy-aware scheduling and server consolidation.

3 METHODOLOGY

PROPOSED SYSTEM METHODOLOGY

To overcome the above limitations, we proposed a new approach in which multi-level security framework in data security mechanism is proposed. It provides uniform simple or high-level security method for all the data in cloud. An adaptive multilevel security framework based on Elliptic Curve Cryptography (ECC) technique that provides adequate security for the classified data stored in cloud. The proposed cloud security system suits well for cloud environment and is also reliant to meet the required level of security of data with different sensitivity that changes with business needs and commercial conditions. It manages to provide adequate level of security for the data classified under different classes.

The proposed approach encompasses suitable access control mechanism, and it provides review control mechanism based on log analysis which facilitates reclassification of data.

PERFORMANCE OF OUR PROPOSED SCHEME

- The proposed encompasses suitable access control mechanism.
- It provides review control mechanism based on log analysis which facilitates reclassification of data.
- It provides multi-level security.
- Changes in the security measures to meet the dynamic changes in cloud security threats.
- Cost and vulnerable for repeated attack is less.
- Provides security based on data sensitivity. An adaptive multilevel security framework based on cryptography techniques that provide adequate security for the classified data stored in cloud.
- Data storage may threaten the sensitive data of users.
- Encrypting Techniques, Various techniques and mechanism was developed to provide security for cloud storage data.
- An efficient way to design hierarchical access control is to use Elliptic Curve Cryptography (ECC).
- Allocate the adequate security algorithm according to sensitive value.

4 MODULES FOR MULTILEVEL SECURITY

4.1) CONSTRUCTION OF CLOUD MODEL

It leverages two different encryption technologies: one is IBE and the other is traditional Public Key Encryption (PKE). First allow a user to generate a first level cipher text under a receiver's identity. The first-level cipher text will be further transformed into a second level cipher text corresponding to a security device. The resulting cipher text can be decrypted by a valid receiver with secret key and security device. Here, one might doubt that this construction is a trivial and straightforward combination of two different encryptions. Unfortunately, this is not true due to the fact that we need to further support security device revocability. A trivial combination of IBE and PKE cannot achieve our goal. To support revocability, we employ re-encryption technology such that the part of cipher text for an old security device can be updated for a new device if the old device is revoked. Meanwhile, we need to generate a special key for the above cipher text conversion. It also guarantees that the cloud server cannot achieve any knowledge of message by accessing the special key, the old cipher text, and the updated cipher text.

4.2) TWO FACTOR DATA SECURITY

The setup phase generates all public parameters and master secret key used throughout the execution of system. The public parameters are shared with all parties participating into the system (including data sender/receiver, cloud server and a PKG), while the master secret key is given to the PKG. The two main factors are SDI and PKG ,that will respectively generate a security device and a secret key for a registered user IDi in secure channel such that the user can combine the security device with the secret key to recover message from its encrypted format.

Cipher text Generation Phase a data sender encrypts a data under the identity of a data receiver and further sends the encrypted data to the cloud server. Knowing public parameters param, a data m ϵ {0,1} k and a receiver's identity IDi, a data sender encrypts a data to a first level encryption. Note the first-level cipher text generation is built on top of Waters IBE. After receiving the first-level cipher text of a data from the data sender, the cloud server generates the second-level cipher text. Knowing public parameters param, a first level encryption for the user, and the information (IDi, tpki) stored in List, the cloud server encrypts C1 = (c1, c2, c3, c4) to a second-level cipher text.

Once a device of a user needs to be updated due to some incidences (e.g. it is either lost or stolen), the user first reports the issue to the SDI. The SDI then issues a new device for the user. Then the SDI notifies the cloud server to update the ciphertext of the user by sending a special piece of information. Finally, a data receiver uses a decryption key and a device to recover the data.

THREE FACTOR MULTI LEVEL DATA SECURITY PROTECTION

In this system, the cloud environment is used to store and retrieve the classified encrypted data by authorized users. Therefore, the data owner outsources only the data and not the entire computations of an organization. Hence, the owner of the data has the opportunity to store the encrypted data in different sections of a bucket or in different buckets at the same location or at different locations as per the service level agreement made between the data owner and the cloud service provider.

Preprocessing Phase

The following steps are carried out by Data Owner (DO):

1. Determining the sensitivity of data based on the security objectives A, I, and C.
2. Classifying the data based on sensitivity value into one of three classes: Class I || Class II || Class III.
3. The adequate security algorithm is identified and encrypting the classified data with different encryption methods.
4. Storing the encrypted data in cloud storage.
5. In this phase we have to Maintain metadata for each data file which contains access privilege, classification type, and mapping data details.
6. The encrypted data are generated and maintained for the future use.

Setup Phase

Data users (DU) register to the DO; DO categorize data users based on the access rights assigned to them.

Data Accessing Phase

1. DU send request to the DO for accessing data.
2. DO verify the user authentication and verifies whether the DU have access privilege to the requested data.
3. DO scrutinizes the request to identify to which class does the requested data belong to and appropriate levels of authentication verifications are done.
4. DO generate token from metadata for accessing the requested data.
5. DO sends the token and secret key to the DU.
6. DU submits only the credentials and token to Cloud Service Provider (CSP) and retain secret key.
7. CSP verifies DU authentication.
8. CSP processes the submitted token to verify the access privilege.
9. CSP retrieves and returns the requested data.
10. DU downloads the requested data.
11. DU decrypts it using secret key.
12. In the setup phase, privilege if data user performs any manipulations, then DU attach digital signature with the modified data.
13. DU stores the modified data into cloud storage.

Key Management Phase

The proposed model assumes that the key stores of both DO and DU remain to be secured throughout the process. DO take the responsibility of generation and distribution of secret keys to DU.

Data Integrity Verification Phase

DO have to periodically verify the integrity of the data stored in cloud to check the correctness of data.

Log Analysis Phase

In cloud storage system we are using log monitoring system, data that needs to be reassessed for its sensitivity value and reevaluation of security measures are identified and are upgraded accordingly.

Token Verification Phase

These steps are executed between CSP and DO when there arise some disputes in the submitted credential and token for data accessing by the DU.

4.4) ALGORITHM FOR PROPOSED METHOD

Step 1: Get the organization data.

Step 2: Analyze data to identify risks.

Step 3: Find the potential impact on cloud data, which is either low, moderate, severe.

Step 4: Based on impact, fix for A, I, and C for each sensitive data.

Step 5: Determine the sensitivity value.

Step 6: Allocate the adequate security algorithm according to sensitive value.

5 ARCHIETECTURE FOR MULTILEVEL SECURITY

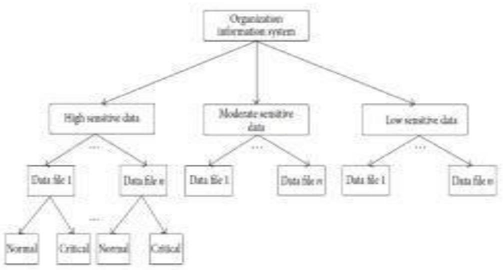


Figure 2 - Data classification archietecture

HIGH SECURITY SCHEME FOR HIGH SENSITIVE CLASS I DATA

The data with high sensitivity value are grouped into Class I. Class I data are highly important and should not be compromised, they require high level security. The high-level security scheme for Class I is a hierarchical access control. An efficient way to design hierarchical access control is to use Elliptic Curve Cryptography (ECC). Three-factor authentication access control for all users with reading and writing privileges. The low level of authentication can be a compromised of factors based on knowledge, token, and biometric schemes (e.g., user password, user security token and biometric identifier). The nature and criticality of the application, the data owner can use biometric authentication; or else it can be replaced with another token-based authentication.

MODERATE LEVEL SECURITY SCHEME FOR NEUTRAL SENSITIVE CLASS II DATA

Moderate and low security objective values are fixed with the highest sensitivity value that is moderate when compared to low and hence such data are grouped into Class II. In Class II, the whole data are with moderate sensitivity and hence to be protected with medium level security scheme. Here also we use hierarchical access control (ECC). The two- factor authentication access control for all users with reading and writing privileges. Each user’s authentication can be a combination of factors based on knowledge and token (e.g., user password, user security token).

BASE LEVEL SECURITY SCHEME FOR LOW SENSITIVE CLASS III DATA

All data with low sensitivity level are grouped under Class III. In Class III, the whole data are require only base line security. Base line security is a combination of base level access control security and simple encryption security for the entire data of this class. Every user’s factor authentication (e.g., user password or any personal identification number) is suggested to access data in Class III. The data can have different security objective value combinations, in general; otherwise, it could be concluded that the highest value among the security objectives should be fixed as the sensitivity level for that data.

6. SECURITY MEASURES TO PROTECT STORED DATA

Measure 1: Access Control. Access control ensures fine- grained access to resources and hence any security system cannot be designed without access control. The specialized mechanism which the access control that controls the flow of data between subject (users, computers, applications, etc.,) and object (computers, applications, files, servers, devices, etc.,) where subject is an active entity that requests access to an object and object is a passive entity that contains the data. For the data prevention, the Unauthorized access to data, either a single access control method or a combination of multiple methods is required. The importance of access control and its relationship to other security services are dealt in [11].

Access control with cryptographic algorithms to all users having the same classification property as that of the requested the resources. To improve the access control model, Mandatory Access Control should be combined with Role Based Access Control (RBAC) which provides the concept of roles or separation of duties. Permissions are assigned to roles and then each user is assigned to a particular role. When a user changes his role, it is enough to revoke his role and no other changes are required. RBAC suits well for cloud environment, one of the mainly used access control [12, 13]. Measure 2: Data Sensitivity. The data classified based on some aspects analysis its sensitivity based on the security objectives availability, integrity, and confidentiality (AIC) which could be followed by data classification. The importance of these security objectives for any data and its potential impacts are well defined in FIPS 199 Publication [8]. Data are separated by the sensitivity value and is considered as the industry standard for computer security which is based on the three important characteristics of data which gives value for its use in organizations: availability, integrity, and confidentiality [9]. Data owner manages the data throughout its lifecycle and must discreetly analyze every data to identify the potential impact on unauthorized disclosure or destruction of that data. Access control impacts due to loss of AIC, the sensitivity value of the data should be fixed.

Measure 3: Classification Plan. There are three types of data classified, namely, high, moderate, or low, based on the values assigned for the security objectives of that data. Following the data classification, appropriate required level of encryption methods should be selected and implemented to protect the classified data.

The AIC table with three classes: high, moderate, and low. The possible combinations of potential impact that any data may possess are shown. Since there are three parameters to be considered each with three impact.

1. Availability, integrity, and confidentiality of data can have minimum value as 1.
2. The value for the impacts high, moderate, and low can have values 3, 2, and 1, respectively.
3. We have to find Sensitivity value by sum of values of all security objectives.

Using the hypothesis, the sensitivity value is determined which ranges from 1 to 9. However, the data can have different security objective value combinations, in general; otherwise, it could be concluded that the highest value among the security objectives should be fixed as the sensitivity level for that data.

To classify data using the hypothesis, that is attributes based on availability, Integrity and Confidentiality.

Step 1. Get the organization data.

Step 2. Analyze data to identify risks.

Step 3. The potential impact on organizational data which is either low, moderate, severe have to find.

Step 4. Based on impact, fix 1,2, 3 for A, I, and C for each data.

Step 5. Determine the sensitivity value.

Step 6: If sensitivity value = 01, then Class =I. If sensitivity value = 02, then Class = II.

If sensitivity value = 03, then Class = III.

Step 7. Allocate the adequate security algorithm.

Measure 4: Data Segmentation. Classification of data based on their sensitivity to the organization. Class I data are concluded to be highly sensitive which requires additional security.

The data in Class I, based on its criticality, can be further segmented to form different partitions. Therefore, after segmentation of data makes the sensitivity get subsided further. Data can be accessed from anywhere and by anyone and in anytime. Data storage may threaten the sensitive data of user's.

7. PERFORMANCE ANALYSIS OF SECURITY ALGORITHMS

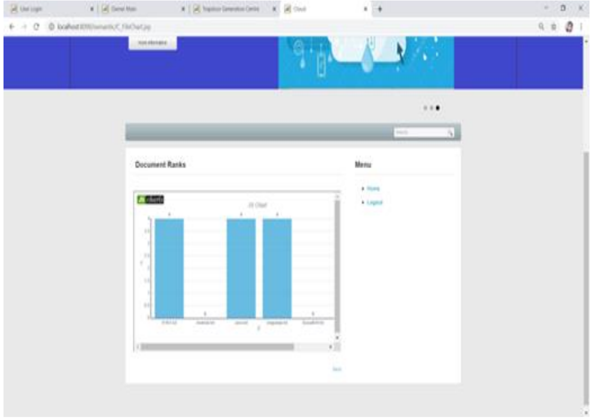
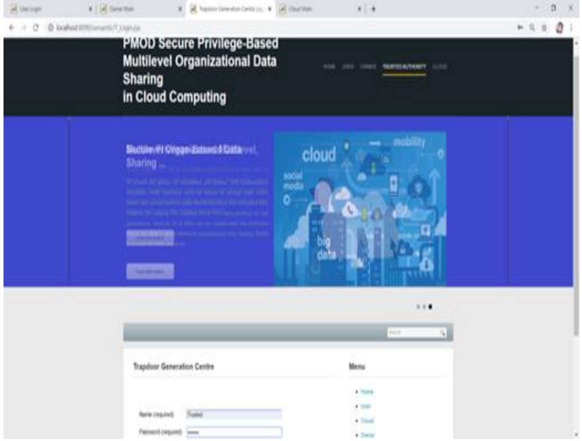


Figure 3 - Performance analysis of security algorithms

Performance Evaluation

The performance of this work is done to prove the performance improvement over the proposed methodology than the existing system in terms of execution time and data confidentiality and File size (MB).

7.1) ENCRYPTED DATA STORED IN CLOUD INSTANCE:


PMOD Secure Privilege-Based
Multilevel Organizational Data
Sharing
in Cloud Computing

Trapdoor Generation Centre

Name (required) Trusted

Password (required) ••••••

Figure 4 - Encrypted data in cloud

This figure displays the encrypted data is stored in cloud storage by the data owner.

8.MULTI LEVEL DATA SECURITY PROTECTION

In this system, the cloud environment is used to store and retrieve the classified encrypted data by authorized users. The main objective of this process is to give high security to the data that is stored in cloud environment. Many techniques are used before for the data security in cloud.

The above survived all the techniques gives security to the cloud data in various ways. From all over the techniques Two factor key generation Technique gives high security than the other techniques.

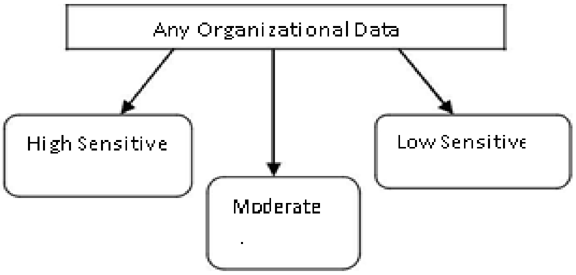


Figure 5 - Data Classification

An adaptive multilevel security framework based on Elliptic Curve Cryptography (ECC) technique that provides adequate security for the classified data stored in cloud. The Multilevel security framework suits well for cloud environment and also more reliant to meet the required level of security of data with different sensitivity. It manages to provide adequate level of security for the data classified under different classes. Once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. MLS can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un decryptable by this device. MLS process is completely transparent to the sender. Therefore, in multilevel security the cloud server cannot decrypt any cipher text at any time.

8.1) ATTRIBUTE COMPARISON

S.NO	Techniques	Security	Efficiency	Access control	Qos, Performance
1	IBE				
2	EDKGR				
3	IBPRE				
4	CCA-Secure				
5	TPA				
6	UCPRE				
7	CLPRE				
8	MUIBPRE				
9	PRE				
10	Two Factor Technique		✓		
11	Multilevel Security Technique		✓	✓	

9 RESULT

9.1) EXECUTION TIME

Execution time is defined as amount of time to complete the process.

12
10
8
6
4
2
0
Execution Time (secs)
Two factors Data security
Multi-level Data security
File size (65 MB)

Figure 6 - Comparison of Execution Time

Figure 3 shows the comparison of execution time between two factor data security mechanism and multi-level data security mechanism.

X axis represents the File size in MB and Y axis represents the execution time in seconds. From the figure 10, it is understood that the proposed Multi level data security mechanism is low than the existing two factor mechanisms.

10 CONCLUSION AND FUTURE WORK

Cloud is well known for its prominent offerings. Organizations interested in data outsourcing opt for cloud storages which satisfy the dynamic business requirements on demand. IIn cloud data security hold back cloud adoption widely. This work proposes a multilevel security framework that is adaptive for cloud environment. The adaptive multilevel security framework proposes to classify the data based on sensitivity and to provide the appropriate required level of security to the classified stored data which is a involving new ideas and methods way to improve and enhance dependent security in cloud system framework environment. The ultimate goal of this adaptive multilevel security framework is to overcome the drawbacks of existing two-level security methods. In this multilevel security system, we used hierarchical access control called Elliptic Curve Cryptography (ECC) which has high performance, low computational cost, and small key size. Based on ECC, hierarchical data access control is designed to fulfill security requirements in cloud environment. Finally, we showed the performance of this work to prove the performance improvement over the proposed methodology than the existing system in terms of execution time and data confidentiality.

In future the proposed work is extended by data classifications followed by different encryption methods are illustrated exhaustively. Access control and key management must be carefully collaborated to preserve the benefits of encryption techniques, because if the secret keys are compromised, there is no meaning in possessing data in encrypted form. Therefore, here if the keys are compromised, then the encrypted data is compromised.

REFERENCES

[1] AWS, "Amazon web services: overview of security process," AWS Security White Paper, 2013.

[2] Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[3] C. Beasley, "Data classification standard," ISO Policies, Stan- dards and Guidelines, The University of Texas at Austin, Austin, Tex, USA, 2011.

[4] C. Beasley, "Data encryption guidelines," ISO Policies, Stan- dards and Guidelines, The University of Texas at Austin, Austin, Tex, USA, 2011.

[5] Chen, H. C., Hu, Y., Lee, P. P., & Tang, Y. (2014). NCCloud: a network-coding-based storage system in a cloud-of-clouds. IEEE Transactions on Computers, 63(1), 31-44.

[6] Chu, C. K., Chow, S. S., Tzeng, W. G., Zhou, J., & Deng, R. H. (2014). Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(2), 468-477.

[7] Cloud Security Alliance, SecaaS Implementation Guidance, Category 8: Encryption. Version 1.0, CSA, 2012.

[8] D. L. Evans, P. J. Bond, and A. L. Bement, "Standards for security categorization of federal information and information systems," FIPS Publication 199, National Institute of Standard and Technology, Gaithersburg, Md, USA, 2004.

[9] D. Markiewicz, Information Security Office-Guidelines for Data Classification, Information Security Policies and Practices, Carnegie Mellon University, Pittsburgh, Pa, USA, 2011.

[10] D. Sudhadevi and K. Thilagavathy, "A novel approach to enhance cloud data defense," Asian Journal of Information Technology, vol. 12, no. 9, pp. 305–311, 2013.

[11] EMC Corporation, "Approaches for encryption of data- at-rest in the enterprise-a detailed review," EMC Software White Paper H4173, 2008.

[12] Ferretti, L., Colajanni, M., & Marchetti, M. (2014). Distributed, concurrent, and independent access to encrypted cloud databases. IEEE transactions on parallel and distributed systems, 25(2), 437-446.

[13] Guo, H., Zhang, Z., Zhang, J., & Chen, C. (2013, October). Towards a secure certificateless proxy re- encryption scheme. In International Conference on Provable Security (pp. 330-346). Springer Berlin Heidelberg.

[14] J. H. Seo and K. Emura. Efficient delegation of key generation and revocation functionalities in identity- based encryption. In E. Dawson, editor, CT-RSA, volume 7779 of Lecture Notes in Computer Science, pages 343–358. Springer, 2013.

[15] K. Kent and M. Souppaya, Guide to Computer Security Log Management, Special Publication 800-92, US Department of Commerce, National Institute of Standard and Technology, Gaithersburg, Md, USA, 2006.

[16] Liang, K., Liu, Z., Tan, X., Wong, D. S., & Tang, C. (2012, November). A CCA-secure identity-based conditional proxy re-encryption without random oracles. In International Conference on Information Security and Cryptology (pp. 231-246). Springer Berlin Heidelberg.

[17] Libert, B., & Vergnaud, D. (2008, March). Unidirectional chosen-ciphertext secure proxy re-encryption. In International Workshop on Public Key Cryptography (pp.360-379). Springer Berlin Heidelberg.

[18] Liu, J. K., Bao, F., & Zhou, J. (2011, May). Short and efficient certificate-based signature. In International Conference on Research in Networking (pp. 167-178). Springer Berlin Heidelberg.

[19] Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2016). Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 65(6), 1992-2004.

[20] M. E. Whitman and H. J. Mattord, Principles of Information Security, India Edition Publications, 2nd edition, 2004.

[21] M. Eltayeb, Understanding users' acceptance of personal cloud computing [Ph.D. Dissertation], Colorado Technical University, Boulder, Colo, USA, 2014, http://search.proquest.com/ docview /1654446716.

[22] M. Green and G. Ateniese. Identity-based proxy re- encryption. In ACNS '07, volume 4512 of LNCS, pages 288–306. Springer, 2007.

[23] R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, 2002.

[24] S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, 2012.

[25] Sahai, A., Seyalioglu, H., & Waters, B. (2012). Dynamic credentials and ciphertext delegation for attribute-based encryption. In Advances in Cryptology–CRYPTO 2012 (pp. 199-217). Springer Berlin Heidelberg.

[26] Shao, J., & Cao, Z. (2012). Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. Information Sciences,206, 83- 95.

[27] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy, O'Reilly Media, Sebastopol, Calif, USA, 2009.

[28] T. Matsuo. Proxy re-encryption systems for identity- based encryption. In Pairing '07, volume 4575 of LNCS, pages 247–267. Springer, 2007.

[29] V. Purohit, "Authentication and access control- the cornerstone of information security," Trianz White Paper, 2008.

[30] Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on computers, 62(2), 362-375.

[31] Y. Jung and M. Chung, "Adaptive security management model in the cloud computing environment," in Proceedings of the 12th International Conference on Advanced Communication Technology, pp. 1664–1669, Busan, The Republic of Korea, February 2010.

[32] Z. M. Yusop and J. H. Abawajy, "Analysis of insiders attack mitigation strategies," Procedia-Social and Behavioral Sciences, vol. 129, pp. 611–618, 2014