International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

A Cloud Storage Prototyping to Simulate Remote Integrity Check without Homomorphic Encryption

Kiran Yadav 1 , Mr. Shailendra Singh Bhalla 2
Sdbct Indore A B Road Rau

Submitted: 02-01-2022 Revised: 09-01-2022 Accepted: 12-01-2022

ABSTRACT—The rapid expansion of the digital needs motivate us to design new and innovative techniques to fulfill the future demands. Cloud computing is one of the most popular computational and storage infrastructure for serving the increasing demand of the computational needs. However the cloud is frequently adopted in a number of applications and also increasing adoption day by day. But the security of data in third party is the main concern of the cloud adoption. In this context a number of research works has been carried out in order to improve the security of the cloud data storage. Therefore the proposed work first involves a review of recent contributions in the domain of cloud data security. In this review we identified that the Homomorphic techniques are much suitable for enhancing the cloud data storage security, but these techniques are much expensive in terms of the time and space complexity. Therefore the proposed technique proposed an identity based cryptographic technique which will not only securing the data on cloud storage and during communication, it also manage and generate keys without disclosing the secrete key to any one. In addition, the method includes the process of integrity check to ensure the secure data exchange among two concerning parties. In order to demonstrate the proposed security concept a prototype of the model has also been prepared. Additionally by using the simulation based experimentation the performance of the proposed model has been measured. The obtained performance of the proposed model demonstrates the proposed technique is efficient and secure for managing the data on cloud without additional computational overhead.

Keywords—cloud storage, identity based cryptography, integrity check, implementation of prototype, performance analysis**.**

I. INTRODUCTION

The cloud computing is one of the reliable and scalable storage and computing service. However it is also secure and offers personalized service but during the data outsourcing and off sourcing there are a risk of security. In this work we aimed to investigate the security aspects of the cloud additionally tried to design a prototype for demonstration of secure data exchange service among two cloud clients.

The cloud is being adopted in almost all the applications in these days. The ability to deal with large amount of data, scalable resource demand and computational ability make it more acceptable. However there are a number of new dimensions of the research and applications are being deployed in the cloud but the cloud infrastructure is still under security threats. This security threats are not directly on the cloud servers because the cloud servers are utilizing higher degree of security and cryptographic techniques to secure the data. But the use of un-trusted and public network during the communication or data delivery the security is the key concern. Security not only impacts on the server storages that impact directly and indirectly entire service infrastructure.

In this context the different researchers are contributed the concept of identity based encryption technique and also utilization of Homomorphic encryption techniques which are relatively much time and memory resource consuming. Therefore the proposed work is motivated to design and develop an efficient cloud data storage security and remote integrity check technique to ensure the security of data in un-trusted networks also. In addition of that the issue of key exchange and their management is also incorporated to prevent the security issues causes by the key leakage. Therefore in order to simulate the proposed methodology for securing the data in cloud or third party storage and communicating the data to an un-trusted network a prototype of the actual Software as a Service (SaaS) application has been proposed for design and implementation.

The aim of the proposed work is to enhance the existing cloud security in terms of data remote integrity check and the time complexity which is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

posses due to the implementation of Homomorphic encryption to prevent the key exchange. Therefore a new model for security and integrity check has been proposed and the following objectives are proposed to work:

1. **To study and explore the domain of cloud data security using the identity based encryption techniques:** this phase of proposed investigative study is performing a review of different identity based cryptographic techniques. Additionally the methods of remote integrity check have also been studied.
2. **To design and implement a secure data and exchange process without Homomorphic encryption:** in this phase the aim is to design and implement a cryptographic security with the remote integrity check with involving the key exchange process to ensure the optimal level of security.
3. **To validate the data remotely and also the performance of proposed prototype model under simulation scenario:** in this phase the data is validated additionally the different performance parameters are also measured for finding the performance of the proposed working model..

II. PROPOSED WORK

The proposed work is aimed to investigate the cloud security concepts and also proposed a cloud security model for ensuring the end to end secure data delivery. This chapter provides the detailed discussion about the various different functional and architectural concepts for designing the proposed cloud security model.

A. System Overview

Recently we have studied different research efforts in the direction of securing the cloud data storage. The key issue in cloud data storage is the security challenges and remote data integrity during outsourcing and off sourcing of data. In this context we have motivated to study about the cloud storage security and validity check. By the obtained literature we have located some interesting points that are sound and effective enough to improve the current security infrastructure of the cloud storage. The identified points are addressed as following to enhance the existing security.

1. The applicable techniques through Homomorphic encryption have a higher computational complexity and communication cost i.e. Pillers algorithm.
2. Requires a secure mechanism for key exchange
3. The third party is assumed as the completely trusted

In order to enhance the model in this study we propose a cloud data storage and validity check infrastructure using cryptographic technique. The basic security architecture is demonstrated in figure 3.1. In this model we have tried to demonstrate the client of the cloud server who wants to exchange some data to another user. Server just picks a file from the sender's machine and delivers to the user. User just directly uses the file. But behind this simple data exchange process we implemented a cryptographically secured data exchange technique. The method is usages a hybrid cryptographic algorithm to encrypt the data for storing into the cloud server. In order to generate the cryptographic key the algorithm combines the identities of sender and receiver, then use the SHA1 algorithm to generate the secure has key. Then utilize the AES encryption algorithm to encrypt the data and store on the server. This key is not given to any one, which is stored on server into a key manager utility.

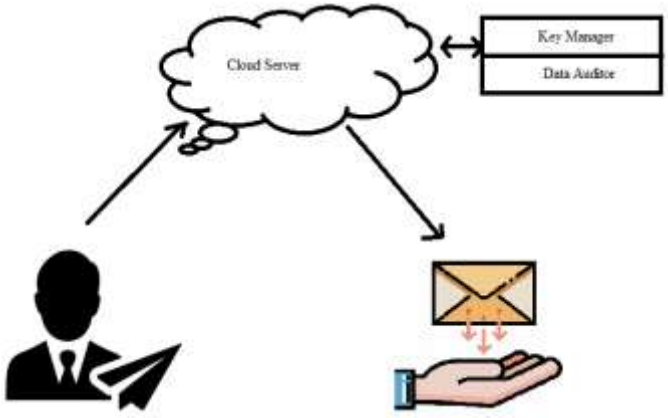

Figure 1 proposed system architecture

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

Therefore, no key is exchanged among any party has been happened. Finally when the data is downloaded at the receiver end server put the secure key for decryption and validation of data integrity. The integrity information is used to validate the data security. Here the data auditor is measure the infection of file, if the data may change more than a threshold. Then the data is not being downloaded from the server due to security measures.

B. Proposed Methodology

The overview of the proposed system architecture has been given in figure 1. The proposed cloud storage security model has been defined and implemented in three modules, namely, cryptographic security, key generation for identity based cryptography, and key management to preserve the key exchange. This section explains the required three modules as:

Cryptographic security

The proposed work is intended to offer the identity based encryption technique. In this concept the cryptographic techniques are used with the identity features of the data owners, additionally the Homomorphic algorithms like pillar algorithm is used. The Homomorphic algorithms are not like the traditional techniques of cryptography. That algorithm generates and use the security key it's owns therefore the algorithm does not require any external input as security parameter. But the major concern is that the Homomorphic encryption algorithm consumes a significant amount of time due to computations.In this context we need to enhance the cryptographic process performance in terms of processing time. Therefore a hybrid cryptographic technique is proposed for implementation as demonstrated in figure2.

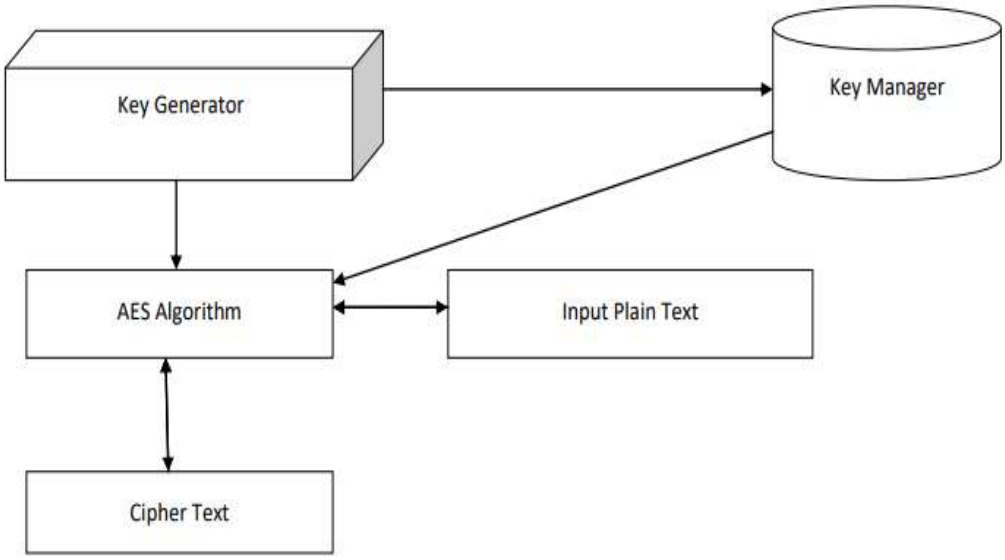

Figure 2 proposed cryptographic infrastructure

The proposed cryptographic model is demonstrated in the above given diagram 2, in this diagram the two components are discussed in the next section. In this section we are just discussing the process of encryption and decryption. The main aim is to reduce the time complexity of the system thus we used the AES algorithm which is secure as well asthe efficient in terms of memory and time complexity. The AES algorithm usage the generated key by the key generator and create cipher text. Additionally to generate the plain text the same infrastructure will be used but the key is obtained by the key manager. In order to describe the encryption process the following step of process will be used as given in table 1.

Table 1 cryptographic system

Input: Cipher Text C, Plain Text P, Key K	
Output: Cipher/Plain Text	
Process:	
1.	if(input == cipher)
a.	$D = AES.decrypt(C, K)$
2.	Else
a.	$D = AES.encrypt(P, K)$

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

3.	End if
4.	Return D

The above given process is used to convert the cipher text to plain text and the plain text to cipher text. The entire model has the tick on key generation phase which is described in next section.

Key Generation

However the key generation process is quite simple but the involved components are different from the other process. The aim is to include the identities of the data owners and also the part of data from the input file. The basic process of the proposed identity based key generation is demonstrated in figure 3. The process is initialized with the capturing the attributes of involved identities among those the file is going to be shared. Here we demonstrate a single party data exchange thus we involved just sender and receiver. In this step the personal identity attributes (based on designer selection) is extracted from the registration database.On the other hand we also are going to include the attribute of the data which is being shared. In this context the proposed model will be utilizing the data and SHA1 algorithm for generating 160 bit hash code. The hash codes are then combined with the other two databases extracted data for generating the final secrete key. The secrete key of the model will be stored in a database which is termed as the key manger. The functional aspects of the key manager are demonstrated in next section.

Key Management

The key manager is a utility which is available on server and used for managing and updating the key for the different sharing scenarios. However the database has three major functions as:

1. **Create new:** when a new file is stored on server, than a new key is derived and stored with the sharing information.
2. **Update:** this will performed when an existing file is shared among more than initial users.
3. **Delete:** this will performed when the data is removed from the server.

In addition, the key is stored in the following format:

Table 2 Key manager storage format

File ID	File Name	Sender	Receiver	Key

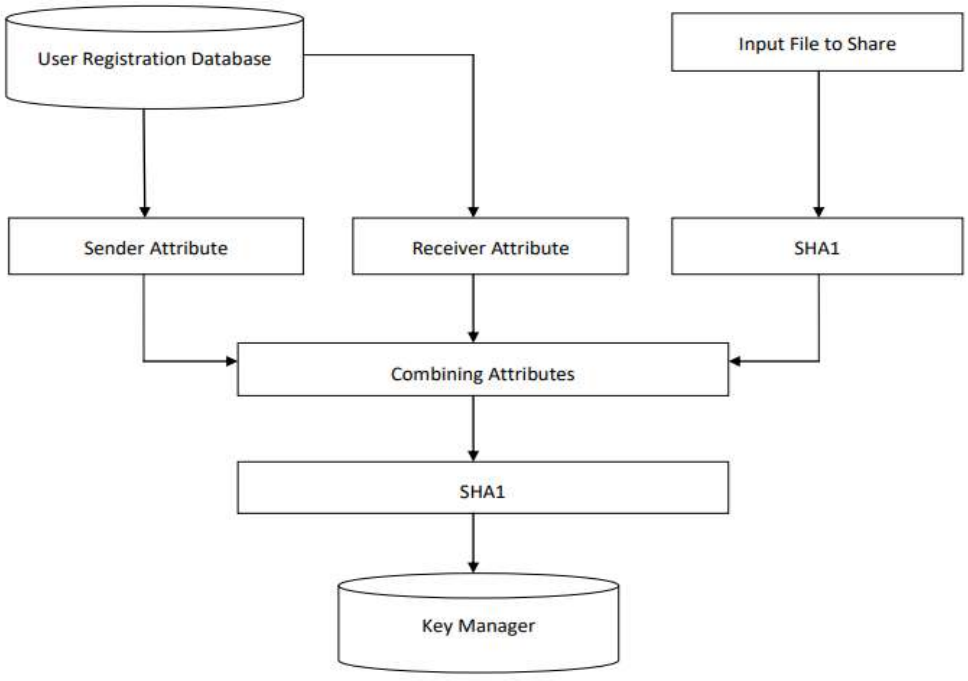

Figure 3 the Key generation module

III. RESULTS ANALYSIS

This chapter provides the evaluation of the proposed secure cloud data storage and sharing model, using the identity based cryptographic technique. The different performance factors are discussed in this chapter.

A. Encryption Time Vs Decryption Time

The time is an essential parameter for evaluating a cryptographic security, the amount of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

time required to encrypt and decrypt the data using the proposed technique is discussed here as encryption time and decryption time. The total amount of time for both the purpose will be measured using the following equation:

$$\text{time consumed} = \text{algorithm finish time} - \text{start time}$$

The measured encryption and decryption time of the proposed cryptographic model and integrity check system is demonstrated in figure 4 and table 3. In order to describe the performance of the system we were used different size of text files for experimentation. In the figure 4 the experimentally used file size is included in the X axis and the relevant time consumed for encryption and decryption process is given in Y axis. The time is measured here in terms of milliseconds (MS).According to the demonstrated results of the encryption time and decryption time we will say the encryption time is less then decryption time, because, during the decryption of the data server need to be evaluate the additional factors for validation of files thus this process increases the time of data decryption.

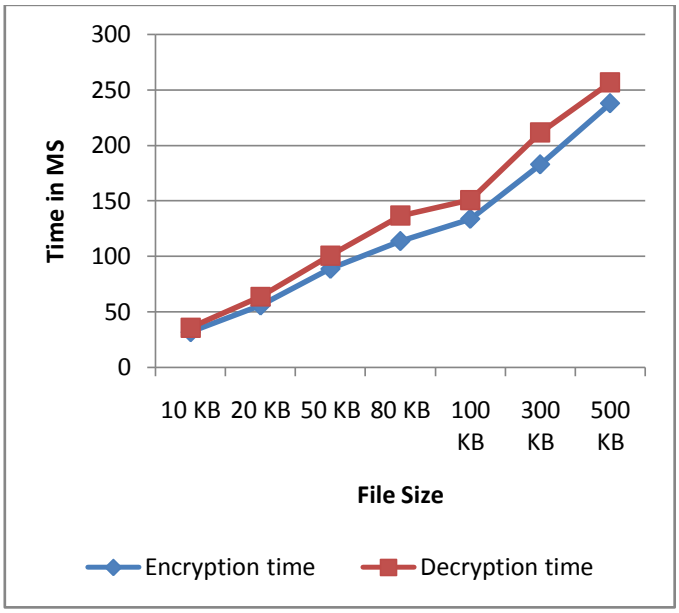

Figure 4 Encryption and Decryption Time

B. Encryption Memory Vs Decryption Memory

The amount of main memory utilized for processing of the data using the implemented algorithm is termed here as memory consumption of the algorithm. The proposed model has developed in the JAVA technology where for measuring the memory usages of the process the following equation will be used:

$$\text{Memory usages} = \text{total assigned} - \text{free space}$$

The observations of the experiments are reported in figure 5 and table 3. In this diagram the memory usages during the encryption of files and decryption of files has been described. The X axis of the diagram shows the file size used in experiments and Y axis shows the memory usages of the algorithms. The memory usages of both the scenarios are calculated in terms of kilobytes (KB). According to the obtained results the performance of the encryption is better than the decryption algorithm.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

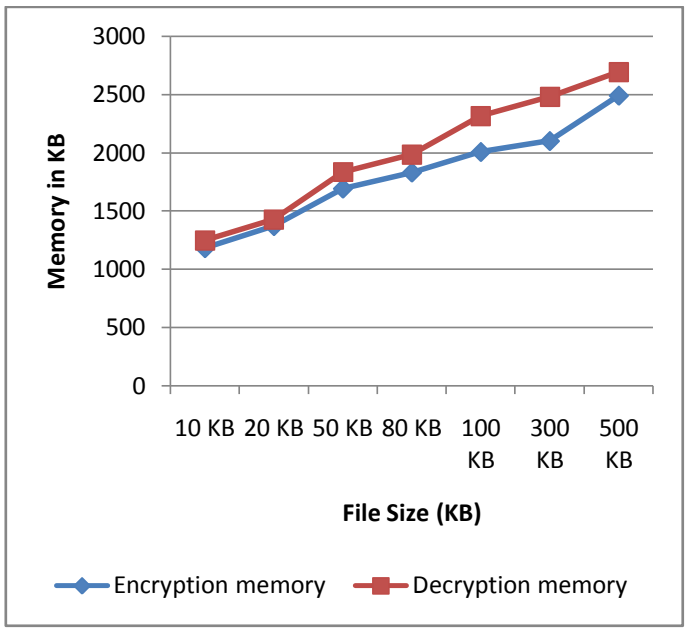

Figure 5 Encryption memory and decryption memory usages

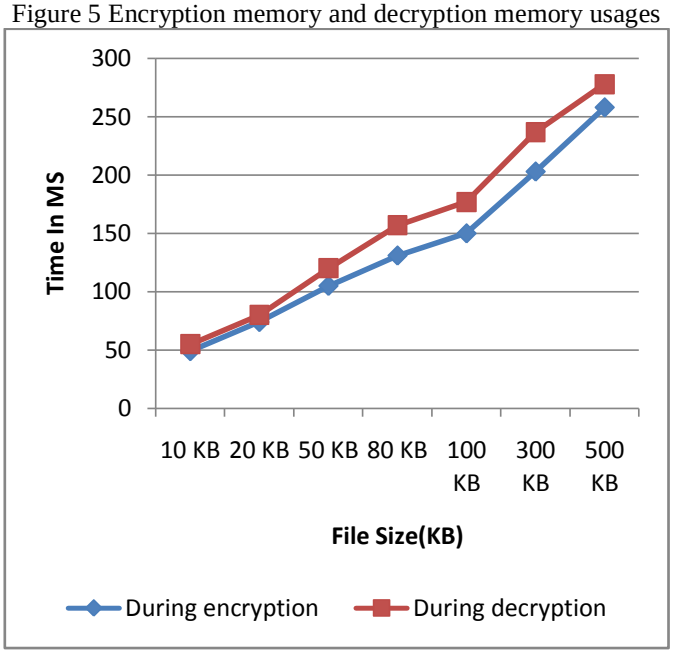

Figure 6 Server Response Time

C. Server Response Time

The server response time is the amount of time which is required to process the client's request. That amount of time includes the time of communication as well as the intermediate operations carried out for processing the data. The server response time is measured using the following equation.

$$\text{reesponse time} = \text{results time} - \text{initilization time}$$

The response time of the server is measured and reported in figure 6 and table 3, the amount of time is measured here in terms of milliseconds (MS). Additionally the response time of the server for both the scenarios are reported i.e. encryption and decryption.In order to demonstrate the performance of the algorithms in both the cases the X axis contains the size of files and Y axis shows the time measured in terms of milliseconds (MS). According to the obtained results the server response time is not much varying from their initial patterns among employ an overhead over the encryption and decryption time approximately 17-25 MS, in the experimental scenarios.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 464-472 www.ijaem.net ISSN: 2395-5252

V. CONCLUSIONS

The main aim of the proposed work is to design and implement an identity based cryptographic technique which will use for securing the data on cloud storage. In this context a security model has implemented and their performance will be estimated. According to the obtained results this chapter provides the conclusion of the work carried out in this study, additionally the future extension of the proposed work has also proposed.

A. Conclusion

The security is one of the major concerns in online services and applications which are carrying the confidential and private data. The intruders and attackers are trying to capture the information from un-trusted networks which will be used for various malicious purposes. In this context the security in network data transfer is an essential part of cyber security infrastructure. However there are a significant amount of work has been contributed in the domain of network and cyber infrastructure but there are very less contributions are available which will work to validate the actual content and the delivered content. Therefore in order to know the possible change in communicated message in network we need a data validation or integrity check model.In this context the proposed work is motivated to design and simulate a secure data storage and exchange model using the cloud computing. In this model we aimed to employ the cryptographic security of the data which is stored on the cloud server. The cryptographic security is employed with the help of two popular cryptographic algorithms namely SHA1 and AES encryption algorithm.

Table 3 Performance of implemented system

File size	Encryption time	Decryption time	Encryption memory	Decryption memory	During encryption	During decryption
10 KB	32	36	1182	1248	49	55
20 KB	56	64	1372	1428	74	80
50 KB	89	101	1694	1837	105	120
80 KB	114	137	1832	1988	131	157
100 KB	134	151	2009	2318	150	177
300 KB	183	212	2103	2481	203	237
500 KB	238	257	2493	2696	258	278

The AES is a symmetric key encryption technique which will use the diverse length of key, additionally the SHA1 algorithm is used for key generation process. The SHA1 considers the user data, sender identity and the receiver identity for generating the secure key. This key will be used for securing the data using AES algorithm as well as it is also used for validating the data at the receiver end. The validation of data at receiver end is known as the integrity check which ensure the quality of data delivered is alter proof or due to some attack or network issues it is being slightly modified.

Table 4 Performance summary

S. No.	Parameters	Description
1	Encryption time	The encryption time is acceptable for the proposed simulation model, additionally increasing with the amount of file s
2	Decryption time	The decryption time is higher than the encryption time due to some additional validation utilities but acceptable.
3	Encryption memory	The memory is directly depends on the amount of data to be processes at the server end
4	Decryption memory	That not has an impact on the local users machine it taken place at the server, which is acceptable for processing the data in large quantity
5	Response time	The server response time is not much affected by the type of process or experiment, which depends on the current server workload. Thus it is slight impact the performance of the proposed model and offer an overhead between 17-25 MS

The proposed identity based secure cloud data storage model simulated using a prototype of the model using JAVA technology and for managing the different factors and keys we will use the MySQL server. Additionally the performance of the proposed based on this simulation has been measured and summarized using table 4.According to the experimental observations we was found that the proposed model is providing the end to end security of data, reduces the risk of data discloser due to leakage of the key in network, and also efficient for processing and sharing the data in cryptographically secured manner.

B. Future Work

The key objectives of the proposed security model has been accomplished successfully, the model is promising and effective for security. In near future for extending the proposed model we suggest the following extensions:

1. Employ some more fine techniques which will efficient encrypt and decrypt the data
2. Identify the hidden identity parameters for providing more secure technique
3. Apply the validation check using the content overlapping in server for identifying the server trustworthiness.

REFERENCES

[1] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, G. Min, "Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information Forensics and Security, 12 (4), 767-778, 2016

[2] I. Foster, Z. Yong, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," in Grid Computing Environments Workshop, 2008. GCE '08, 2008, pp. 1-10

[3] M. Armbrust, "Above the Clouds: A Berkeley View of Cloud Computing," Univ. California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb. 2009.

[4] M. Sookhak, "Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues." ACM Computing Surveys, 47.4 (2015): 65.

[5] J. F. Yang, Z. B. Chen, "Cloud Computing Research and Security Issues," 2010 IEEE International Conference on Computational Intelligence and Software Engineering, Wuhan pp. 1-3

[6] "Introduction to Cloud Computing", Dialiogic, available online at: https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf

[7] T. Mather, S. Kumaraswamy, S. Latif, "Cloud security and privacy: an enterprise perspective on risks and compliance", "O'Reilly Media, Inc.", 2009.

[8] J. T. Goulding, "Identity and Access Management for the Cloud: CA Technologies strategy and vision", Tech. Rep. May, CA Technologies, 2010.

[9] S. Pearson, "Taking account of privacy when designing cloud computing services", Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing IEEE Computer Society, 2009

[10] N. Rawat, R. Srivastava, "Data Security Issues in Cloud Computing", Open Journal of Mobile Computing and Cloud Computing, Volume 1, Number 1, August 2014

[11] V. S. K. Maddineni, S. Ragi, "Security Techniques for Protecting Data in Cloud Computing", Master Thesis, Electrical Engineering November 2011

[12] J. Harauz, L. M. Kaufman, "Data Security in the World of Cloud Computing"

[13] S. Obrutsky, "Cloud Storage: Advantages, Disadvantages and Enterprise Solutions for Business", (2016).

[14] J. Wu, "Cloud storage as the infrastructure of cloud computing", 2010 International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), IEEE, 2010.

[15] "Cloud Storage", Nonprofit Technology Collaboration, available online at: http://www.baylor.edu/business/mis/nonprofits/doc.php/197132.pdf

[16] L. O Akingbade, "Cloud Storage problems, benefits and solutions provided by Data De-duplication", International Journal of Engineering Science and Innovative Technology, Volume 5, Issue 6, November 2016

[17] "What is Cloud Storage?" available online at: https://aws.amazon.com/what-is-cloud-storage/

[18] "Introduction to Cryptography", available online at: http://www.ggu.ac.in/download/Class-Note14/public%20key13.02.14.pdf

[19] G. C. Kessler, "An Overview of Cryptography", 30 June 2010

[20] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid", 7th IEEE International Conference for Internet Technology and Secured Transactions, London, UK, December 2012

[21] C. Hongbing, R. Chunming, T. Zhenghua, Z. Qingkai, "Identity Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing", Chinese Journal of Electronics Vol.21, No.2, Apr. 2012

[22] J. Li, Jingwei Li, X. Chen, C. Jia, W. Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing", IEEE Transactions on Computers Vol: 64 No: 2 Year 2015

[23] J. Yu, and Huaqun Wang, "Strong Key-Exposure Resilient Auditing for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, 2016

[24] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, R. Buyya, "Ensuring Security and Privacy Preservation for Cloud Data Services", ACM Comput. Surv. 49, 1, Article 13, 39 pages, DOI: http://dx.doi.org/10.1145/2906153

[25] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, K. K. R. Choo, "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems", Journal of Latex Class Files, Vol. 14, No. 8, August 2015

[26] N. Dottling, S. Garg, "Identity-Based Encryption from the Diffie-Hellman Assumption", c International Association for Cryptologic Research 2017, CRYPTO 2017, Part I, LNCS 10401, pp. 537–569, 2017.

[27] P. Gaborit, A. Hauteville, D. H. Phan, J. P. Tillich, "Identity-Based Encryption from Codes with Rank Metric", c International Association for Cryptologic Research 2017, CRYPTO 2017, Part III, LNCS 10403, pp. 194–224, 2017.

[28] K. Lee, "A generic construction for revocable identity based encryption with subset difference methods", PLoS ONE 15(9): e0239053. https://doi.org/10.1371/journal.pone.0239053

[29] C. Meshram, C. C. Lee, S. G. Meshram, M. K. Khan, "An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment", Soft Computing Springer-Verlag GmbH Germany, part of Springer Nature 2019