Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210257

Data Confidentiality in Cloud Storage. A Survey

Shekhar S Kausalye [a,1], Dr. Sanjeev Kumar Sharma [a]
[a] *Dept. of Computer Science and Engineering, Oriental University, Indore, INDIA*

Abstract. In cloud computing security, privacy and data confidentiality plays important role when popularity in terms of cloud computing services is consider. Till now there are various schemes, protocols and architecture for cloud computing privacy and data protection are proposed which are based on data confidentiality, cryptographic solution, cipher text blocks, various transforms, symmetric encryption schemes, attribute-based encryption, trust and reputation, access control, etc., but they are scattered and lacking uniformity without proper security logic. This paper systematically reviews as well as analyze research done in this relevant area. First various shortcomings in cloud computing, architectures, framework and schemes proposed for data confidentiality will be discussed; then existing cryptographic schemes, encryption functions, linear transform, grid storage system, key exposure, secret sharing, AONT (All or Nothing Transform), dispersed storage, trust, block encryption mechanism, attribute-based encryption, access control will be discussed; thirdly propose future direction with research challenges for data confidentiality in cloud computing; finally focus is on concern data confidentiality scheme to overcome the technical deficiency and existing schemes.

Keywords. Cloud Computing, AONT, ciphertext, key exposure, dispersed storage, dataconfidentiality.

1. Introduction

The notion of utility computing, grid computing and distributed computing forms basis of Cloud Computing. In this concept extremely vast amount of computing, storage and networking resources along with software resources work together to form a group of virtually unlimited shared resources.

In Cloud Computing, owner of data is not aware about where their data is stored and that is why they are not having control over it which is being executed on the cloud platform. It can be said that the user does not know whether data is secured or not is there any kind of security is provided or not. To implement, use and deliver cloud computing technology owner of data must trust third party called CSP (Cloud Service Provider), now here comes the security, privacy, confidentiality, and trust problems despite of that SOC reports of CSP are reviewed by organizations in timely manner.

[1] Dept. of Computer Science and Engineering, Oriental University, Indore, INDIA
E- mail. shekhar_sk@hotmail.com.

There are many schemes available for privacy protection, based on encryption, block cipher, access control, secret sharing schemes, key exposure, trust but all of them are not scattered and not in symmetry [1]. It makes us to think on the recent results in various technologies for data confidentiality and privacy protection in cloud computing. As promising as it could be, cloud computing is additionally confronting numerous difficulties which, if not settled, may obstruct its quick and innovative development. Information security, it occurs in numerous different applications, is amongst these difficulties that would raise extraordinary worries from the client's side when client store their valuable or private data on cloud service providers server or called it as cloud server. These worries start from the way that cloud servers are normally controlled or handled by business suppliers or commercial cloud service provider which are probably going to be outside trust domain of the clients or users. In a few pragmatic application frameworks, information privacy is not just a security or protection issue but may be juristic concerns. For instance, in medical care application situations use and divulgence of ensured well- being data should meet the necessities of Health Insurance Portability, Responsibility Act, keeping client information secret against the cloud server is not only an alternative, however it is a necessity.

Re-appropriating information to cloud servers are beneficial because of economy, versatility, and availability, however critical specialized difficulties remain there alongside these benefits. Sensitive and delicate information stored in the cloud should be shielded from being perused by a cloud supplier that is straightforward honest yet inquisitive or curious. Step by step as the innovation expands the aggressors additionally be- come ground-breaking such assailants break the information classification by obtaining key by unapproved way. When the key is uncovered, information is lost.

Key openness is one genuine security issue for cloud storage framework or system. The review incorporates those security plans which settle the key openness issue in broadens. Existing encryption modes, methods, schemes and issues related to cloud are available which are discussed here.

2. Key Issues

Distributed computing organizations state that information is secure, however it is too soon to be totally certain about that. Cloud security concerns emerging because both client information and program are stored in cloud service provider's premises. While cost and convenience are two incredible benefits of cloud computing but has key security concerns that must be managed when thinking about shifting basic products and sensitive information to public and shared cloud conditions.

2.1 Cloud Data Security

To address drawbacks of cloud data security, the cloud service provider should create adequate controls and security policies to give the equivalent or a more noteworthy security. Security of information and confidence issue has constantly a vital and challenging issue in Cloud Computing [2]. It bases over improving security by utilizing

OTP confirmation framework, information confidentiality by employing hash calculations and mix data naturally with the most noteworthy solid or quick encryption calculation which guarantee the immediate recovery of information. To guarantee rightness of client information in cloud computing, first, client should be verified by means of various confirmation or authentication means. Authentication is one of the ways toward approving or affirming that credential given by a client are significant and valid.

2.2 Cryptography

Cryptography is the study of utilizing math to scramble and unscramble information. It is the specialty of securing data by changing the first message, called plaintext into an encoded message, called a code or cipher text. It empowers you to store sensitive data or on the other hand send it over insecure network so it cannot be perused by anybody aside from the proposed beneficiary. There are two unique sorts of cryptography which are private key cryptography and public key cryptography. In Private key cryptography a similar key is utilized for both encryption and decoding. Model for private key cryptography are AES, Blowfish, DES and Caesar Code. Out in the open key cryptography, two keys are required, one for encryption and one for decoding. Model for public key cryptography are RSA and YAK [3].

2.3 Advanced Encryption Standard

AES i.e., Advanced Encryption Standard works on block cipher having size of 128 bits for encryption and decryption as well. It is a block cipher. Input to AES is 128 bits of block of data and a key which then processes and at output ciphertext is generated. Size of key decides the various number of rounds that can be performed by AES. The larger the number of rounds more will be data secure. But one problem with a greater number of rounds to encrypt the data is it will increase the time but having one advantage that it is improved than the exhaustive key search attack.

2.4 CPA-Encryption andSecret-sharing

It is combination of the Chosen Plaintext Attack secure encryption with secret-sharing. When file is encrypted then it is shared with n-out-of-n secret-sharing scheme, then it is (n-1) CAKE secures as well as ind secure. Sharing of the encryption key then distributing it across different storage servers located at different geographical location with the ciphertext is not secure when we consider an ind-attacker. If the adversary is having access of all servers where data is stored and is able to download all ciphertext blocks, then adversary can also download all the key shares and stored along the ciphertext blocks to calculate final encryption key.

2.5 All-or-nothing Encryption

This is not encryption and does not required decryptor to have any mystery key. This shows that, All-or-nothing is not secure compared to an ind. One option is to combine the use of All-or-nothing with standard encryption. Rivest proposes pre-measure of a message with an AONT and subsequently scramble its yield with an encryption mode. This perspective is suggested in the composition as All-or-nothing encryption and gives (n-1) CAKE security. Current AON encryption plans need in any occasion two rounds of square code encryption with two keys. At any rate one round is required for the genuine All-or-nothing change that introduces the essential encryption key in pseudo-ciphertext. New encryption key is used in another round which guarantee CPA security. Regardless, two encryption changes set up a critical overhead while encoding and unscrambling gigantic reports. These game plans are either not pleasant as far as security is considered or achieve an enormous overhead when diverged from Bastion and might not be appropriate to store tremendous archives in a multi-dispersed capacity framework.

Table 1. Comparison of survey paper

Survey Work	Year	Technology Covered	Research Work
This Work	2020	Cloud Computing	Data Confidentiality, encryption
[4]	2013	Cloud Computing	Policy and encryption
[5]	2017	Cloud Computing	Side Channel
[7]	2015	Cloud Computing	Encryption
[14]	2019	Cloud Medical	Encryption
[15]	2018	Healthcare	Cloud Searchable Encryption
[16]	2019	E-health	Cloud Encryption

3. Related Work

Here the focus in on reviewing security and privacy in cloud computing, and rather involves related areas, like edge and fog computing, Blockchain and IoT. The comparison is shown in Table 1.

In academic Cloud computing security is the imp and hot topic for discussion. [4] has studied 5 security and privacy attributes which are confidentiality, integrity, availability, accountability and privacy. Also, their relationship has been demonstrated, but the main missing point is lack of specific performance comparison and description. [5] stated various schemes for secret communication, some of which are side channel attack and secret channel, along with their advantages and disadvantages.

F. Cai et. al. [6] reviewed cloud computing key security and privacy challenges, they have classified the existing solutions, also compared their advantages and disadvantages. The only missing point was comparison with the other articles [7] which is based on cloud in medical field is a novel computing model for medical which focuses on challenges of electronic health reword abbreviated asHER.

R. Zang et. al. [8] reviewed four technologies. attribute-based encryption with keyword search, public key encryption with keyword search, searchable symmetric encryption and proxy re-encryption in terms of technical review only. K. Edemacu et. al. [9] discussed about various attribute-based electronic health encryption schemes. Security, efficiency and revocation ability was compared and analyzed. But privacy protection technology discussed is relatively single.

M. Abd-el-Malek et. al. [10] proposed the lattice-based encryption algorithm for hardness of Ring Learning with Errors problem, to make it secure against the files which is stored in Cloud Storage. Lattice based encryption is cryptography techniques which is used to impede attack by both conventional and quantum computers. Using Lattice Based Cryptography technique files are not under attack when compare with another public- key techniques like RSA or Diffie Hellman. [11] are centering to endure the expanding number of fault-tolerant utilizing the deficiency, administrations without critical abatement in execution. This is accomplished by question/update protocol with the assistance of Byzantine fault-tolerant service.

Desai [12] proposed that when Blowfish algorithm is combined with AES it im- proves data security which is stored on the cloud. Symmetric cipher algorithm i.e., Blow- fish is used for the security of data and encryption. Block size of encryption is 64 bit and has a variable key length from 32 bits up to 448 bits. It has much better cost and security, time complexity compared to encryption based on Hierarchical Attribute Set. In the Advanced Encryption Standard used for encryption of electronic data, user can encrypt and decrypt the files and images with less amount of time. This ensures end to end secure communication of data without any unscrupulous data. Future scope may consist of to encrypt video and generate a stronger encryption algorithm which takes very less time and less memory.

Xiaojun Zhang et al. [13] introduced the public auditing scheme for identity based key exposure from lattices as key exposure is serious security issue in cloud auditing services. They studied few cloud auditing schemes addressing key exposure based on pairing and realized the common problem in all of those that these are not secure from quantum attacks also these relies on complex certificate management which is in Public Key Infrastructure (PKI). So, to overcome these problems they proposed a quantum resistant and independent of PKI scheme which depends on lattice assumption in cloud storage.

Chengyu Hu et al. [14] has discussed about auditing of cloud storage with key exposure resilience in continual key leakage. Forward security is provided by various researchers to address the key exposure problem. In this the lifetime of secret key is divided into various periods and then updating the key in these periods. This assures the validity of authenticators before the secret key is fully exposed. But the security of this protocol can be broken using side channel attack in which the secret key is not fully leaked instead it is leaked partially.

4. Research Gap

The level of the cloud storage security is enhanced by using various encryption algorithm which are combined with the integrity verification scheme. Storage selection phase is divided into three sections which are Hybrid, Private and Public. IDEA, AES, SAES and Blowfish technique are implemented. Data is encrypted using AES under Private section after which SHA-1 (Secure Has Algorithm) is applied on the encrypted data to generation 16-digit integrity verification code. This code is attached with the encrypted file or data before it has been stored in the cloud storage. Once the data is stored then SHA-1 is again applied to generate the unique token for the user having 16 digits, this token helps user to access their data stored on the cloud. In Public section Blowfish encryption algorithm is used to encrypt the data with rest of the things are like that of private section. To adhere the data confidentiality encryption is used now a days. But main problem with the confidentiality and encryption is its secret key, which if get exposed or leaked it will create major risk to the data stored in cloud. To counter this the only way is to restrict the access to the encrypted data. If dispersed cloud storage is used the main advantage is data is spread or stored on multiple servers located at different geographical locations with different admin domain. The novel method which was proposed is named as bastion which is claimed as efficient and fast compared to the existing schemes. The scheme uses only one bock cipher encryption round and then linear transform, which make it (n-2) cake. This ensures that plain text will not be recover on the condition that adversary is having all but two cipher-text blocks, this will be applicable when key is leaked. One of the major challenges in the data confidentiality in the cloud is cryptographic keys. Once the key is leaked or exposed, data confidentiality can be only preserved by limiting the attacker's access to the cloud data i.e., cipher text block. But all the existing work focus on the cryptographic key security and distributing the encrypted data over various servers in the network. But the attacker with proper keying material can compromise one of the servers and is able to decrypt the ciphertext block stored there. Also, current system requires pre-processing of block cipher encryption as well as another round of block cipher encryption which reduces the system performance.

5. Proposed Work

In addition to all above various schemes and technologies, the more secure and complete system which is standardized should be formed. In future, research challenge remains there like combining the various algorithms, increasing the strength of the key, increasing block cipher encryption, storage system and so on. So, considering these challenges in future a proposed system combines the bastion scheme with linear transform and more secure cipher algorithm which can overcome the key exposure problem and address the data confidentiality with less system overhead.

An All or Nothing Transform (AONT) is a capable of processing change which maps progressions of information or data to succession of blocks which are generated which has properties like. (i) given all generated blocks, change can be capably inverted, and (ii) everything except from one of the yield blocks, it's difficult to Figure any unique data. Proposed future system will ensures security of the plaintext even if attacker has the encryption key and has few blocks. Current plan requires a pre-taking care of round of

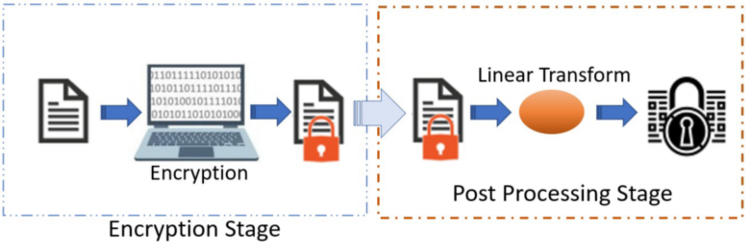

Figure 1. Proposed System uses Encryption along with Linear Transformation

block-cipher encryption for the AONT, trailed by next round of encryption. In an unforeseen manner, proposed system as shown in Figure 1., at first scrambles the data with first round of encryption, and by then applies a capable straight post processing to ciphertext. Subsequently, algorithm loosens up the thought of All-or-Nothing encryption. Algorithm uses block encryption in the CTR mode with irregular Key K. Proposed future system will ensures security of the plaintext even if attacker has the encryption key and has few blocks. Current plan requires a pre-taking care of round of block-cipher encryption for the AONT, trailed by next round of encryption.

In an unforeseen manner, proposed system as shown in Figure 1., at first scrambles the data with first round of encryption, and by then applies a capable straight post processing to ciphertext. Subsequently, algorithm loosens up the thought of All-or-Nothing encryption. Algorithm uses block encryption in the CTR mode with irregular Key K.

6. Conclusion

In the vast area of web and internet there are strong chances that your data may get exposed or leaked. So main concern in digital world is how to protect the security and confidentiality in the cloud computing. In this paper various cryptographic schemes, methods are addressed which tried to solve the problem of key leakage, data confidentiality and security. When all the schemes mentioned in this paper are analyzed and studies it has been observed that proposed system becomes more effective which can be achieved by using an efficient modified block cipher encryption followed by linear transform with very minimum system overhead when compared to all other schemes. Proposed system is suitable where data is stored on different cloud storage server which make it difficult for advisory to acquire all the blocks of data to decipher it in case of key leakage.

Acknowledgment

Authors are thankful to Department of Computer Science and Engineering, Oriental University, Indore for their contentious supports. This work also been supported by Department of Information Technology, Sanjivani College of Engineering, Kopargaon.

References

[1] C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, “Robust data sharing with key-value stores,” in Proceedings of the 30th annual ACM SIGACT-SIGOPS symposium on Principles of distributed com- puting - PODC ’11. ACM Press, 2011.

[2] V. Padmapriya, J. Amudhavel, M. Thamizhselvi, K. Bakkiya, “A scalable service-oriented consistency model for cloud environment (SSOCM),” in Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015) - ICARCSET ’15. ACM Press, 2015.

[3] J. Amudhavel, S. Kumarakrishnan, B. Anantharaj, D. Padmashree, S. Harinee, and K. P. Kumar, “A novel bio-inspired krill herd optimization in wireless ad-hoc network (WANET) for effective routing,” in Proceedings of the 2015 International Conference on Advanced Research in Computer Science

Engi- neering & Technology (ICARCSET 2015) - ICARCSET ’15. ACM Press, 2015.

[4] P. G. Shynu and K. J. Singh, “A comprehensive survey and analysis on access control schemes in cloud environment,” Cybernetics and Information Technologies, vol. 16, no. 1, pp. 19–38, mar 2016.

[5] M. S. Inamdar and A. Tekeoglu, “Security analysis of open-source network access control in virtual net- works,” in 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, may 2018.

[6] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, “Survey of access control models and technologies for cloud computing,” Cluster Computing, vol. 22, no. S3, pp. 6111–6122, feb 2018.

[7] J. Ni, K. Zhang, X. Lin, and X. Shen, “Securing fog computing for internet of things applications. Challenges and solutions,” IEEE Communications Surveys & Tutorials, vol. 20, 601–628, 2018

[8] R. Zhang, R. Xue, and L. Liu, “Searchable encryption for healthcare clouds. A survey,” IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 978–996, nov 2018

[9] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, “Privacy provision in collaborative ehealth with attribute-based encryption. Survey, challenges and future directions,” IEEE Access, vol. 7, 89 614–89, 2019.

[10] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, “Fault-scalable byzantine fault-tolerant services,” in Proceedings of the twentieth ACM symposium on Operating systems principles - SOSP ’05. ACM Press, 2005

[11] N. Jayapandian, A. Z. Rahman, R. Sangavee, and R. Divya, “Improved cloud security trust on client-side data encryption using HASBE and blowfish,” in 2016 Online International Conference on Green Engineering and Technologies (IC-GET). IEEE, nov 2016

[12] A. Desai, “The security of all-or-nothing encryption. Protecting against exhaustive key search,” in Advances in Cryptology — CRYPTO 2000. Springer Berlin Heidelberg, 2000, pp. 359–375

[13] Xiaojun Zhang, Huaxiong Wang, Chunxiang Xu, “Identity-based key-exposure resilient cloud storage public auditing scheme from lattices”, Information Sciences, Vol. 472, pp. 223-234 2018

[14] Kumar, A., Vengatesan, K., Vincent, R., Rajesh, M., & Singhal, A. (2019). A novel Arp approach for cloud resource management. International Journal of Recent Technology and Engineering (IJRTE), 7(6).

[15] Chengyu Hu, Yuqin Xu, Pengtao Liu, Jia Yu, Shanqing Guo, Minghao Zhao., “Enabling Cloud Storage Auditing with Key-Exposure Resilience under Continual Key-Leakage”, Information Sciences, 2020