Data Security using Secured Key Protocol in Cloud Computing

[1]Maddi Vedh, [2]Praveena P
[1,2]Dept. of Computer Science and Systems Engineering, Andhra University Autonomous College of Engineering, Visakhapatnam, AP, India

Abstract
In Cloud computing innovation there isapractice of critical strategy issues, which incorporate issues of protection, security, namelessness, broadcast communications limit, government reconnaissance, unwavering quality, and obligation, among others. Be that as it may, the most imperative between them is security and how cloud supplier guarantees it. Encryption is an outstanding innovation for securing touchy data. This paper exhibits an outline of security issues and furthermore breaks down the plausibility of applying encryption calculation for data security and protection in cloud Storage. It likewise attempted to cover the different algorithms utilized by specialists to take care of the open security issues. In this paper we have talked about cloud computing security issues, component, challenges that cloud service supplier look amid cloud building and introduced the figurative investigation of different security algorithms.

Keywords
Cloud Computing, Access Control, Data proprietors, Cloud Storage, Assemble Director, Amass Client

I. Introduction

Cloud computing is a worldview that gives huge control edge and tremendous memory space requiring little to no effort. It empowers clients to get planned services independent of time and area over different stages (e.g., cell phones, PCs), and in this way conveys extraordinary accommodation to cloud clients. Among various services given by cloud computing, cloud storage service, for example, Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a more adaptable and simple approach to share data over the Internet, which gives different advantages to our general public. Be that as it may, it additionally experiences a few security dangers, which are the essential worries of cloud clients. Right off the bat, redistributing data to cloud server infers that data is out control of clients. This may cause clients' wavering since the re-appropriated data as a rule contain important and touchy data. Furthermore, data sharing is frequently actualized in an open and antagonistic condition, and cloud server would turn into an objective of assaults. Surprisingly more dreadful, cloud server itself may uncover clients' data for unlawful benefit. Thirdly, data sharing isn't static. That is, the point at which a client's approval gets lapsed, he/she should never again have the benefit of getting to the beforehand and accordingly shared data. Accordingly, while re-appropriating data to cloud server, clients likewise need to control access to these data with the end goal that just those as of now approved clients can share the re-appropriated data. A characteristic answer for vanquish the issue is to utilize cryptographically upheld get to control, for example, identity based encryption (IBE). The idea of integrity based encryption was presented by Shamir, and helpfully instantiated by Boneh and Franklin. IBE wipes out the requirement for giving an open key framework (PKI). Despite the setting of IBE or PKI, there must be a way to deal with renounce clients from the framework when vital, e.g., the expert of some client is terminated or the mystery key of some client is uncovered. In the customary PKI setting, a few procedures are generally affirmed, for example, authentication repudiation list or affixing legitimacy periods to endorsements. Nonetheless, there are just a couple of concentrates on repudiation in the setting of IBE. Boneh and Franklin initially proposed a characteristic renouncement route for IBE. They added the current day and age to the Cipher Text, and nonrevoked clients occasionally got private keys for each day and age from the key expert. Tragically, such an answer isn't adaptable, since it requires the key specialist to perform direct work in the quantity of non-disavowed clients. Also, a safe channel is fundamental for the key expert and non-denied clients to transmit new keys.

II. Related Work

Yong Yu (2016) et. al exhibited solid development from RSA mark can bolster variable-sized document squares and open inspecting. Here give a formal security model to IDCDIC and demonstrate security of our development under RSA presumption with immense open types in arbitrary prophet model. We exhibit the introduction of our proposition through building up a model of the convention. Usage results present that proposed ID-CDIC convention is pragmatic and adoptable, all things considered, [3]. M. Vijayalakshmi (2016) et. al introduced an instrument known as "programmed mending of services in a Cloud computing air" in which server downs are maintained a strategic distance from and thus, saving message misfortune. To forestall message misfortune at the season of server crashes, we actualized a system of two distinct folds. One is observing methodology running on Port/PID, checking CPU, Disk and memory inside occurrence and getting separate activities. Another is computerizing methodology made reference to in the initial step. While observing, we became more acquainted with which service achieves CPU usage 90%. At that point programmed resume of such service happens, maintaining a strategic distance from server downs. One more commitment of our paper is clients can depict their very own principles dependent on which activities will be activated concurring need. We executed our system in AWS cloud where Cloud Watch is the observing apparatus. In like manner the proposed system can be executed in any of the clouds. Contrasted and the past endeavors, our procedure is compelling and yields enhanced results [9]. Mohammed Amoon (2016) et. al introduced a versatile structure to the adapt issue of adaptation to non-critical failure in Cloud computing environment. The system utilizes both replication and check directing methodologies all together toward gain a solid stage for completing client demands. Likewise, calculation decides the most fitting adaptation to internal failure method for each chose virtual machine. Recreation test is completed to assess system's execution. The results of the analyses present that proposed system improve cloud execution in states of throughput, overheads, financial expense, and accessibility [2]. Abderrahim El Mhouti (2016) et. al exhibited that in this paper, through exploiting Cloud computing services, we propose to plan an adaptable cloud-based

VCLE. The fundamental objective of this proposed work abuse Cloud computing possibilities to encourage communitarian data development and boost asset partaking in VLE. The proposed stage satisfies fundamental VLE prerequisite to help communitarian adapting, yet additionally reacts to student's dynamic need on interest. The stage encourages and underpins understudies to satisfy assignment driven learning in an extra adaptably and inviting shared way [1]. Peidong Sha (2016) et. al displayed that, we plan an encoding approach, this encoding approach right off the bat separates whether private and open key qualities produced at the season of the encoding method contain prime number, at that point joins with the Pascal's triangle hypothesis and RSA calculation model and inductive system to develop another cryptosystem that meets homomorphic calculation of a few activities on cihpertexts (e.g., increases, duplications), Thus the novel cryptosystem fulfills totally homomorphic encryption in (CC) [10]. Mr.V.Biksham (2016) displayed a high security encoded data is proposed applying "fairly" and "completely homomorphic" encryption system. CSP give security and protection to the cloud clients by cryptographic encryption algorithms. Through applying inquiry any client would information be able to access from cloud servers through unscrambling. Be that as it may, visit decoding of figure content may prompt adventure the honesty and verification. To furnish security to encoding data with algorithms, a protected encryption approach known as homomorphic encryptions which gives estimations on encoding data without decode figure message and enhance cloud services performance [3]. Nitin Naik (2015) et. al exhibited a working model and basic examination of these three open standard character conventions SAML, OIDC and OAuth. It likewise investigates assessment criteria which are utilized for this examination reason. All in all, it examines their impediments and qualities, and set up most fitting open standard personality convention for different types (CC)models [4].

III. Collusion Attack Scheme

Because additive embedding method [8] is widely used in watermarking, average attack is used as a main security analysis tool. This section describes collusion attack which extends average attack so as to enable k traitors to create a pirate image of good quality safely. For self-contained, the average attack is introduced in the following.

A. Average Attack

Trappe et al. studied the security of AND-ACC fingerprinting based on the collusion attack model in [9] as

$$\begin{cases} \hat{\mathbf{Y}} = \sum_{i=1}^{k} \lambda_i \mathbf{Y}_i \\ \lambda_1 + \lambda_2 + \cdots + \lambda_k = 1 \\ 0 \le \lambda_i \le 1 \qquad\qquad i = 1, 2, \cdots, k \end{cases} \tag{1}$$

where Y_i is the legal watermarked image of traitor P_i, i = 1,2,⋯ ,k = 2r+1. Trappe et al selected λ_i = 1/k, and they also noted: "there may exist cases in which the underlying fingerprints will not necessarily have the same energy, or be independent of each other, and that other choices for λ_i might be more appropriate." Although Trappe et al. noticed the existence of other collusion attacks, they did not propose an effective collusion attack but average attack. Indeed, Su et al. [8] extended the average attack. They noted "more sophisticated linear temporal filters by allowing β_k (i.e., λ_i in [7]) to take on arbitrary values". Clearly, their collusion is not right. For example, if β_k = 100, the traitors will obtain nothing but noise according to Su's attack [9]. Thus, How to select λ_i is very important in the linear attack. In the following, a collusion attack model is addressed.

B. Linear Combination Collusion Attack

Collusion Attack extends the average collusion attack [9][7] by removing the unnecessary restraint $0 \le \lambda_i \le 1$ from formula (1), and the updated attack model is

$$\hat{Y} = \sum_{i=1}^{k} \lambda_i Y_i \tag{2}$$

$\lambda_1 + \lambda_2 + \cdots + \lambda_k = 1$

Generally speaking, all the watermarks have almost the same energy. In order that each traitor has the same probability of escaping from being identified, the contribution to the pirated image from any traitor should be almost identical. That is to say, $|\lambda_1| = |\lambda_2| = \cdots = |\lambda_k|$. Hence, λ_i is selected to be 1 or -1 in the collusion attackof the present paper. Without loss of generality, the collusion attackmodel is

$$\hat{Y} = -\sum_{i=1}^{r} Y_i + \sum_{i=r+1}^{2r+1} Y_i. \tag{3}$$

Obviously, the challenge for collusion attackis how to achieve good fidelity of the pirated image. To quantitatively describe the similarity between the original image **X** and the pirated image $\hat{\mathbf{Y}}$, suppose the processing image is 8-bit gray images, and all the independent watermarks have the same energy, calculate the PSNR (peak signal-noise-ratio) as

$$\begin{aligned} \sigma^2 &= \frac{1}{n^2} \| \hat{\mathbf{Y}} - \mathbf{X} \|^2 = \frac{1}{n^2} \| \sum_{i=1}^{k} \lambda_i \mathbf{Y}_i - \mathbf{X} \|^2 \\ &= \frac{1}{n^2} \| \sum_{i=1}^{k} \alpha \lambda_i \mathbf{W}_i \|^2 = \frac{k}{n^2} \| \alpha \mathbf{W} \|^2 . \\ PSNR &= 10(\lg 255^2 - \lg \sigma^2) \\ &= 10(\lg 255^2 - \lg \frac{1}{n^2} \| \alpha \mathbf{W} \|^2) - 10 \lg k \\ &= PSNR_0 - 10 \lg k, \end{aligned}$$

Where $PSNR_0$ is the PSNR of the original watermarked image. Comparing with PSNR of the original watermarked images, the PSNR of the pirated image is decreased only 10lgk dB. For instance, if there are three traitors, the PSNR of pirated image is reduced 10lg3=4.7dB.

IV. Cloud Security Controls

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:

A. Deterrent Controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

B. Preventive Controls

Preventive controls strengthen the system against incidents,

generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

C. Detective Controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[8] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

D. Corrective Controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

V. Security and Privacy

A. Identity Management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customers identity management system infrastructure, using federation or SSO technology, or a biometric-based identification system,[1] or provide an identity management solution of their own.[3] CloudID, for instance, provides privacypreserving cloud-based and cross-enterprise biometric identification solutions for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.

B. Physical Security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

C. Personnel Security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive

D. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted, as shown in figure, and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

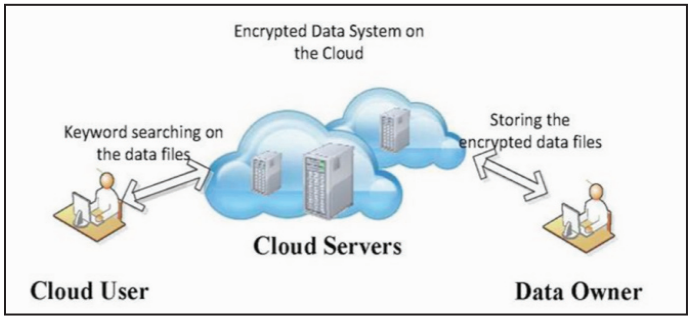

Fig. 1: Encrypted Data System on the Cloud

VI. Data Security

There are a number of security threats associated with cloud data services, not only covering traditional security threats, e.g network eavesdropping, illegal invasion, and denial of service attacks, but also including specific cloud computing threats, e.g., side channel attacks, virtualization vulnerabilities, and abuse of cloud services. To throttle the threats the following security requirements are to be met in a cloud data service [4].

A. Data Confidentiality

Data confidentiality is the property that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

B. Data Access Controllability

Access controllability means that a data owner can perform the selective restriction of access to his data outsourced to cloud. Legal users can be authorized by the owner to access the data, while others cannot access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

C. Data Integrity

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated.

If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

VII. Proposed System

The group manager will maintain the revocation list of the members. If any of the member leave the group then the member detail is added to that list and the user will not be able to further login to that group. When the new member is added to the group then group key is provided to the member. To remove identity privacy problem, the group manager will have the list of the uploaded files along with the memberID from which the file is uploaded. By this privacy is kept secure and no one will misuse as it is traceable by the group manager. And as it is multi-owner then any member can

not only read data but also modify their own data along with the group manager. The files which are uploaded present in encrypted form, and the files can be viewed by group member as they have the group key on which he or she belongs.

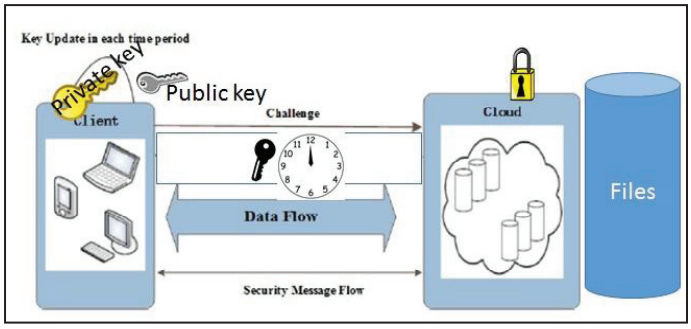

Fig. 2: Proposed System Architecture

A. AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix.

The AES Encryption consists of four different stages they are:

- **Substitute Bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
- **Shift Rows:** A Simple Permutation
- **Mix Columns:** A substitution that makes use of arithmetic overGF(9)
- **Add Round Key:** A Simple Bitwise XOR of the current block with the portion of the expanded key

B. AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

VIII. Conclusion

Cloud computing is an emerging technology. It is an attractive solution when the infrastructure or the IT personnel are not available or too expensive; but it has its drawback. The disadvantage can be mostly found in the secure threats and cloud computing vulnerabilities. Unlike classical solutions where threats come from two known sources inside or outside the network; Cloud computing security threats might originate from different sources. In this paper define about cloud deployment models, cloud computing service delivery models, characteristic of cloud, risks of adopting cloud computing, technology, security issues in cloud and data encryption using RSA, DES and AES.

IX. Future Work

Cloud computing is relatively a new and widely emerging domain and it must have to overcome the security issues in order to be more and more prominent technology of the future. A lot of research is being done in this regard to solve these major issues but still many problems are unseen and unknown and the doors for future research are always open.

References

[1] Zhongma Zhu, Rui Jiang,"A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia,"A View of Cloud Computing", Comm. ACM, Vol. 53, No. 4, pp. 50-58, Apr. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003. Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Shucheng Yu, Cong Wang, Kui Ren, Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] R. Lu, X. Lin, X. Liang, X. Shen,"Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 6, pp. 1182-1191, 2013.

[7] D. Boneh, X. Boyen, E. Goh,"Hierarchical Identity Based Encryption with Constant Size Ciphertext", Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] Lan Zhou, Vijay Varadharajan, Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, pp. 1947-1960, 2013.

[9] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge,"Cloud Computing: A Perspective Study, New Generation Computing- Advances of Distributed Information Processing", Vol. 28, Issue 2, pp. 137-146, 2010.

[10] Puneet Jai Kaur, Sakshi Kaushal,"Security Concerns in Cloud Computing, Communication in Computer and Information Science", Vol. 169, pp. 103-112, 2011.

Maddi vedh is presently pursuing M. Tech (CNW) Department of computer science and engineering from Andhra University, Visakhapatnam, AP, India.

Praveena P, M.Tech is working as an SWT(Subject-Wise Teacher) in the Department of Computer Science And Systems Engineering, Andhra University College of Engineering, Visakhapatnam, AP, India.