International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Integration of Data Confidentiality in Cloud Computing

K. Prathyusha[1], K. Aproova[2], Ch. Bhavani[2], G. Ghireesh Goud[2]

[1]Assistant Professor, Department of Information Technology in Teegala Krisha Reddy Engineering College,Telangana, India

[2]UG Scholar, Department of Information Technology in Teegala Krisha Reddy Engineering college, Telangana, India

ABSTRACT

Data confidentiality by acquiring cryptographic keys, bymeans of coercion or backdoors in cryptographic software are maintained in every level of access. Once the encryption key is exposed, the only viable measure to preserve data confidentiality is to limit the attacker's access to the ciphertext. This may be achieved, for example, by spreading ciphertext blocks across servers in multiple administrative domains—thus assuming that the adversary cannot compromise allot them. Nevertheless, if data is encrypted with existing schemes, an adversary equipped with the encryption key, can still compromise a single server and decrypt the ciphertext blocks stored therein. In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the ciphertext blocks. We analyze the security of data, and we evaluate its performance.

Keywords : Cipher Text, Data Confidentiality.

I. INTRODUCTION

Data is encrypted and dispersed across different administrative domains, an adversary equipped with the appropriate keying material can compromise a server in one domain and decrypt cipher text blocks stored therein. One preprocessing round to create the data, followed by another round for the actual encryption. Notice that these rounds are sequential, and cannot be parallelized.

Cloud and virtualization gives you agility and efficiency to instantly roll out new services and expand your infrastructure. But the lack of physical control, or defined entrance and egress points, bring a whole host of cloud data security issues – data co-mingling, privileged user abuse, snapshots and backups, data deletion, data leakage, geographic regulatory requirements, cloud super-admins, and many more.

Virtualization and cloud computing require cooperation between security, storage, server, application, and cloud security admins – all with access to your most sensitive data. With this number of people, the risks of failing an audit, or an admin going rogue, grow exponentially.

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud

providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).[3] The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance report, insider attacks are the sixth biggest threat in cloud computing.[4] Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.[2]

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware – be it computing, storage or even networking. This introduces an additional layer – virtualization – that itself must be properly configured, managed and secured.[6] Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Cryptographically secure pseudo random number generator of Blum et al. that enables the mobile client to efficiently retrieve the result of the computation, as well as to verify that the evaluator actually performed the computation. We analyze the server-side and client-side complexity of our system.

II. OBJECTIVE

DIFFERENT DATA SECURITY TECHNIQUES

1. Homomorphism token pre-computation technique.
2. File distribution preparation.
3. Token pre- computation.
4. Challenge token function and error localization.

Figure 1 : Basic terminology of secure data.

Defining some terms used in Cryptography:
Plaintext is the original intelligible source information or data that is input to algorithms x Cipher text is the scrambled message output as random stream of un intelligible data.
Encryption Algorithm substitutes and performs permutations on plain text to cipher text x Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
Keys are used as input for encryption or decryption and determines the transformation.

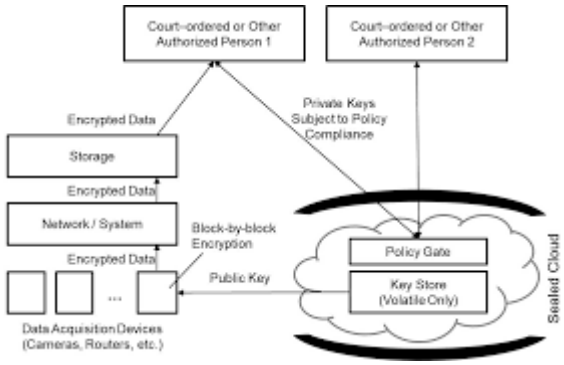

Figure 2 : Encrypted data at remote area and storage in cloud.

Sender and Recipients are persons who are communication and sharing the plaintext.

Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.

Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.

Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.

Secure Stored Data: question mark on controlling the encrypt Tion and decryption by either the end user or the Cloud Service provider.

User Access Control: for web based transactions (P CI DSS), web data logs need to be provided to compliance auditors and security managers.

III. IMPLEMENTATION

Encryption & Decryption Time: This is calculated as the time required for encryption which involves converting the plain text payload file into cipher text. The authors used the encryption time to find the through put which indicated the computation cost i.e. the encryption speed. The decryption time is calculated for the amount of time required for converting the cipher text back into the plain text.

Cloud Providers are giving more focus on having end user data as secure as possible and having low priority for cloud performance due to inconsistent selection of algorithms for encryption and encoding. By selecting the right cryptographic scheme end user data security can be achieved without losing out on cloud performance.

In case a third person gains access to the secure secret key, cipher text messages can easily be decrypted. The fact of having one single secret key algorithm is the most critical issue faced by Cloud service providers when dealing with end users who communicate over unsecure internet. The only option is to have that secret key be changed often or kept as secure as possible during the distribution phase.

Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.

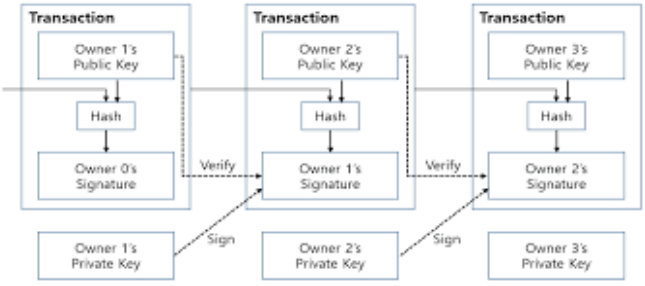

Figure 3: Hash function for secure data for one transation.

Problem confirming if the content is altered or actually sent by the claimed sender .If a hacker has the secret key, decrypting the cipher text, modifying the information being sent with that key and send to the receiver. Since a single key is involved during the

crypto process, either side of the transactions can get compromised.

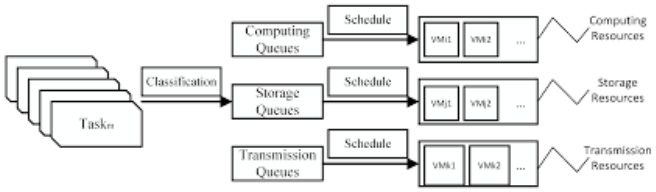

Figure 4 : data storage strategies at remote areas.

Cryptanalysis where the attacks are focused on the characteristics of the algorithm to deduce a specific plaintext or the secret key. Then hacker s are able to figure out the plaintext for messages that would use this compromised setup.

The proposed which will prevent the cloud infrastructure in three main places, in client location, in the network and in server. This cryptographic security system is designed in such a way so that computation time for decryption of cypher text messages for the hackers will be more compared to any single cryptographic system.So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments and storage (databases hosted by the Cloud provider). The concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider.

IV. CONCLUSIONS

With Cloud computing emerging as a new in thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. This makes Cloud security considering the data storage at remote areas of the cloud environment. Use of security algorithms and ensuring these are implemented for secure cloud data storage and needs to be properly utilized in order to ensure end user security.

V. REFERENCES

[1]. M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Re-iter, and J. J. Wylie, "Fault-Scalable Byzantine Fault-Tolerant Services," in ACM Symposium on Operating Systems Principles (SOSP), 2005, pp. 59–74.

[2]. M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in International Conference on Dependable Systems and Networks (DSN), 2005, pp. 336–345.

[3]. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, "Security amplification by composition: The case of doubly-iterated

[4]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM , Apr. 2010.

[5]. E. Barker et al. Recommendation for key management – part 1: General (revision 3). NIST Special Publication 800-57 , July 2012.

[6]. D. Beaver, S. Micali, and P. Rogaway. The round complexityof secure protocols. InACM STOC'90.

[7]. A. Ben-David, N. Nisan, and B. Pinkas. Fairplaymp: A system for secure multi-party computation. InACM CCS, 2008.

[8]. L. Blum, M. Blum, and M. Shub. A simple unpredictablepseudo random number generator.SIAM J. Comput., 15(2):364–383, May 1986.

[9]. S. Bugiel, S. Nurnberger, A.-R. Sadeghi, and T. Schneider. Twin clouds: Secure cloud computing with low latency. InProc.CMS, 2011.

[10]. M. Burkhart, M. Strasser, D. Many, and X. Dimitropou-los. Sepia: Privacy-preserving aggregation of multi-domain network events and statistics.In Proceedings of the 19th USENIX Conference on Security , USENIX Security'10, pages 15– 15, Berkeley, CA, USA, 2010. USENIX Association.

[11]. H. Carter, B. Mood, P. Traynor, and K. Butler. Secure out-sourced garbled circuit evaluation for mobile devices.InUSENIX Security, 2013.

[12]. I. Damgard, V. Pastro, N. Smart, and S. Zakarias. Multiparty computation from somewhat homomorphic encryption.In Advances in Cryptology–CRYPTO 2012, pages 643–662. Springer,2012.

[13]. J. Domingo-Ferrer. A provably secure additive and multiplica-tive privacy homomorphism. InProc. Int'l Conf. on Information Security, 2002.

[14]. Y. Duan, J. Canny, and J. Zhan.P4p: Practical large-scale privacy-preserving distributed computation robust against malicious users. In Proceedings of the 19th USENIX Conference on Security , USENIX Security'10, pages 14–14, Berkeley, CA, USA, 2010. USENIX Association.

[15]. R. Gennaro et al.Non interactive verifiable computing: Outsourcing computation to untrusted workers. In CRYPTO 2010.

[16]. C. Gentry. Computing arbitrary functions of encrypted data. Commun. ACM , Mar. 2010.

[17]. O. Goldreich.Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, 2004. 15O. Goldreich, S. Micali, and A. Wigderson. How to play anymental game. InACM STOC , 1987.

[18]. S. Goldwasser et al. Reusable garbled circuits and succinct functional encryption. In ACM STOC'13