An Analysis of Confidentiality Management in Cloud Computing

Ms. Preethi P [*1], Dr. Asokan R [#2]
[*1] Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India,
[#2] Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India,

***Abstract*:- The computational world is becoming very large and complex. Cloud Computing has emerged as a popular computing model to support processing large volumetric data using clusters of commodity computers. With the fast development of computing and communication technique, a high-quality of information area unit generated. Over the last years, cloud computing satisfies the applying necessities and grows terribly quickly. Basically, it takes the information process as a service, like storage, computing, information security, etc. However, along with desirable benefits come risks and security concerns that must be considered and addressed correctly. The investigation of potentials for secret communication in cloud environments and its possible application scenarios are needed. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. Thereby, the current approaches of different kinds of secret communication including covert channels, side channels and obfuscation techniques have to be reviewed. This paper highlights and categorizes many of security issues introduced by the "cloud"; surveys the risks, threats and vulnerabilities, and makes the necessary recommendations that can help promote the benefits and mitigate the risks associated with Cloud Computing.**

Keyword:* *Cloud Computing, Cloud security, Network level security, Covert Channels, Deduplication, Service-level agreements, Interoperability.

1. INTRODUCTION

Along with the fast development of computing and communication technique, a high-quality of information area unit generated. These large information desires additional study computation resource and bigger space for storing. Over the last years, cloud computing satisfies the applying necessities and grows terribly quickly. Basically, it takes the information process as a service, like storage, computing, information security, etc. The cloud users utilization in general public cloud platform reduced the problems in storage management and information access over geographical locations. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The advantages of using cloud computing are: i) reduced hardware and maintenance cost, ii) accessibility around the globe, and iii) flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter. The paradigm of cloud computing is based on an offer of "Different kinds of secret communication including covert channels, side channels and obfuscation techniques" [1]. A plethora of definitions have been given explaining the cloud computing. Cloud Computing has been defined as the new state of the art technique that is capable of providing a flexible IT infrastructure, such that users need not own the infrastructure supporting these services. This integrates features supporting high scalability and multi-tenancy. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. According to the different types of services offered, cloud computing can be considered to consist of three layers. IaaS or Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service. PaaS – the Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. SaaS - Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand[2] SaaS ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" [3]. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.

A public key cryptosystem because of the absence of PKI, the revocation drawback could be a essential issue inIBE settings. Many voidable IBE schemes are projected on this issue.

SaaS - Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand[2] SaaS ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock" [3]. Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS).

Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance.

In the **Platform as a service approach (PaaS)**, the offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons.

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information.

2.BARRIERS TO CLOUD COMPUTING

In spite of being a hot topic, there are certain aspects behind the fact that many organizations are

yet not confident of moving into the cloud. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats. A few issues limiting the boundaries of this transformational concept are:

2.1. Privacy and Security

The fundamental factor defining the success of any new computing technology resides on the term how much secure it is. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or it is more secure to store the data away from cloud in our own personal computers or hard drives? At-least we can access our hard drives and systems whenever we wish to, but cloud servers could potentially reside anywhere in the world and any sort of internet breakdown can deny us access to the data lying in the cloud. The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately stored. There have been instances when their security has been invaded and the whole system had been down for hours. At-least half a dozen of security breaches occurred last year bringing out the fundamental lapses in the security model of major CSPs. With respect to cloud computing environment, is defined as "the ability of an entity to control what information it reveals about itself to the cloud/cloud SP, and the ability to control who can access that information".[11] discusses the standards for collection, maintenance and disclosure of personality identifiable information. Information requiring privacy and the various privacy challenges need the specific steps to be taken in order to ensure privacy in the cloud as discussed in [4].

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, supporting middleware [13] etc. The security of the cloud depends on the behaviour of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users is increasing, security risks are getting more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection. Because of the multifarious security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to public cloud in future if needed.

Emergence of cloud computing owes significantly to mashup. A mashup is an application that combines data, or functionality from multiple web sources and creates new services using these. As these involve usage of multiple sub-applications or elements towards a specific application, the security challenges are diverse and intense. Based on this idea, a secure component model addressing the problem of securing mash-up applications. Also, privacy needs to be maintained as there are high chances of an eavesdropper to be able to sneak in.

2.2. Data Storage over IP Networks

Online data storage is becoming quite popular now-a-days and it has been observed that majority of enterprise storage will be networked in the coming years, as it allows enterprises to maintain huge chunks of data without setting up the required architecture. Although there are many advantages of having online data storage, there are security threats that could cause data leakage or data unavailability at crucial hour. Such issues are observed more frequently in the case of dynamic data that keeps flowing within the cloud in comparison to static data. Depending upon the various levels of operations and storage provided, these networked devices are categorized into SAN (Storage area network) and NAS (network-attached storage) and since these storage networks reside on various servers, there are multiple threats or risks attached to them. The three threat zones that may affect and cause the vulnerability of a storage network.

Besides these, from them a mobile cloud computing scenario, we may see that unlike cloud computing there are several additional challenges that need to be addressed to enable MCC reach its maximum potential:

Network accessibility: Internet has been the major factor towards the cloud computing evolution and without having the network access it won't be possible to access the internet and hence the inability to access the mobile cloud limiting the available applications that can be used.

2.3 Different Search Schemes of Searchable Encryption

A. Public Key Encryption with Keyword Search (PEKS)

Dan Boneh et al. [6] first proposed the scheme of public key encryption of keyword search (searchable encryption). 'Public Key Encryption with Keyword Search' scheme is an example of Asymmetric Searchable Encryption Scheme. The construction of their scheme consists of four randomized algorithms as stated above. The scheme is secured against Chosen Keyword Attack (CKA) assuming Billinear Diffie-Hellman Problem (BDH) is intractable. In their scheme, they have showed that the scheme of searchable encryption implies the scheme of Identity based encryption (IBE).

B. Extension of PEKS scheme

Michel Abdalla et al. [15] identified and filled some drawbacks of the scheme of searchable encryption (SE) introduced in [5] in 2007. Compared to the scheme of Boneh et al.[15] is statistically consistent. The combination technique of IBE and PEKS is showed in their paper. They have proposed a well defined identity based encryption with keyword search scheme (IBEKS). Their scheme is IND-CPA secure.

C. Deterministic and Efficiently Searchable Encryption (DESE)

This scheme is proposed by Mihir Bellare et al. in 2007 [15]. The scheme is deterministic and bucketization technique is used here. The use of SE scheme in remote database server is briefly described in the paper.

D. Symmetric Searchable Encryption (SSE) As stated above there are mainly two type of constructions of SE scheme, one is symmetric searchable encryption and another one is asymmetric searchable encryption. The first scheme of symmetric searchable encryption was proposed by Song et al. [1], search time of the scheme is linear to size of dataset. A security definition of symmetric searchable encryption scheme was well defined by Goh et al. [3] and their scheme was proposed with bloom filter. In two scheme on SSE, SSE-1 and SSE-2 was designed by Curtomola et al. The main advantage of their scheme is that the scheme is privacy preserving and provide optimal search time. SSE-1 is secure against CKA1 (chosen keyword attack) and SSE-2 is secure against CKA2 (adaptive chosen keyword attack). However, in SSE every time sender requires a secret key from receiver that leads to a complicated key management

E. Fuzzy Keyword Search As stated above searchable encryption suffers from Keyword Guessing Attack (KGA), to overcome this problem Peng Xu et al. [15] introduced a scheme of SE which is secure against KGA. Despite of a single trapdoor function, they used two keyword search trapdoor in their mechanism, i.e fuzzy keyword search trapdoor (Ftw) and exact keyword search trapdoor (Etw). In the construction of fuzzy keyword search trapdoor one or more keyword can be mapped to the same fuzzy keyword search trapdoor, so that if the adversary get to know the search trapdoor he/she can not understand the correct decryption of the keyword. Thus the scheme ensures privacy against KGA even if the keyword space is in polynomial size. In the implementation of the scheme [15] the public-private key pair are generated by the user. User also computes F tw and Etw. After getting F tw from the user, search operation is performed by the storage server and a set of most matching ciphertexts of the query keywords is returned to the user. Then the exact test is performed by the receiver of the query with Etw to evaluate the exact search of the query.

3. LEAST EXPLORED AREAS OF CLOUD SECURITY

Though, Cloud data location had always been a highly debated issue, no fruitful research has yet been conducted in this field. A client who is storing her valuable data or hosting her applications on the Cloud, remains unaware of it's original location as already discussed in section 3.1.1. Suitable location based access control models are yet to be designed for overcoming such problems. Moreover, ample research for introducing proper access control methodologies suitable for the cross-domain or multidomain [15] of Cloud is yet to be done. Again mutual trust between the CSP and the Client is another vital issue that is inevitably related to cloud security. Though the works of (Hwang, Li, 2010 [13]) based on Reputation systems (for CSP trust evaluation) and that of (Li-qin Chuang, Yang, 2010 [14]) for user trust evaluation are some of the few in this domain, a rigorous study and research in this area is expected to be done in the near future. Data or service compliance is another complicated issue when it comes to Cloud computing. Since, ultimately the organizations are responsible for the security and privacy of data held by the CSP on their behalf, proper construction of the SLA policies and following a specific jurisdiction by the CSP becomes neccessary. Lack of collaborative work between the cloud user and the CSP in identifying and reacting to security incidents is another vital area of cloud security that need to be explored in-depth.

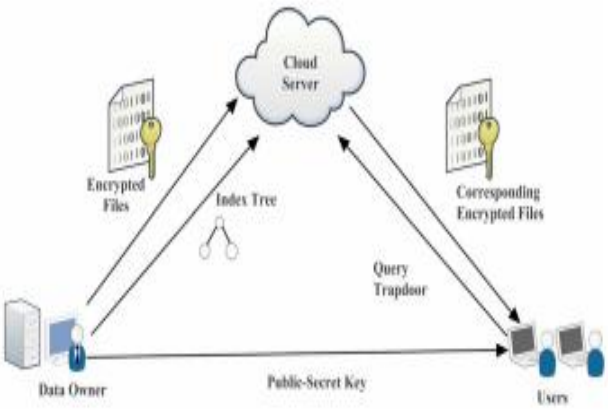

Figure 1: System Model of the Scheme

S.No.	Title	Author	Issue	Method Used	Tools	Advantage	Disadvantage
1.	Privacy-Preserving Public Auditing for Secure Cloud Storage.	Cong Wang Sherman S.M. Chow Kui Ren.	Users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing.	Privacy preserving Public auditing protocol method.	C and cloud server side in Amazon Elastic Computin g Cloud (EC2)	Scheme enables an external auditor to audit user's cloud data without learning the data content.	CSP might hidedata loss incidents to maintain a reputation.
2.	Robust Remote Data Checking.	Reza Curtmola Osama Khan.	The integration of Forward Error Correction (FEC) codes with remote data checking schemes that rely on spot Checking.	The forward error-correcting encoding method.	Monte-Carlo simulation model- C++	Protection against corruption of a large portion of File. Theclient will detect with high probability if the server corrupts more than a - fraction of file.	These data checking protocols are asymptotically less efficient.
3.	Aggregate and Variably Encrypted Signatures from Bilinear Maps.	Dan Boneh Craig Gentry Ben Lynn HovavShacha m.	Signature constructions using generic gap Diffie-Hellman group.	Aggregate signatures with bilinear maps.	Java	Aggregate signatures usefulfor reducing the size of certicate chains and for reducing message size in secure routing protocols.	Security of the system in a model that gives the adversary choice of public keys and messages to forget.
4.	Improving Privacy and Security in Multi- Authority Attribute- Based Encryption.	Melissa Chase Sherman S.M. Chow.	The trusted cen- tralauthority, GIDcomprom ises the privacy of the user.	Attribute Based Encryption Scheme.	Java	Removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular Users.	In a multi-authority ABE scheme, multiple attribute- authorities monitor different sets of attributes and issue corresponding decryption Keys to users.
5.	Chosen-Ciphertext Secure Proxy Re-Encryption	Ran Canetti Susan Hohenberger y	Re-encryption scheme achieved only semantic security. IN contrast, applications often require security against chosen ciphertext attacks.	Proxy re-encryption scheme using Decisional Bilinear Diffie-Hellman(CCA-secure PRE)	Proxyenab led Chefs file system	PRE schemes that are secure in arbitrary protocol settings, Or in other words are secure against chosen ciphertext attacks	It is often not sufficient to guarantee security in General protocol settings
6.	Improved Proxy Re-Encryption Schemes with Application s to Secure Distributed Storage	Giuseppe Ateniese Kevin Fu	BBS Scheme which is transitive and bi-directional	Proxy re-encryption technique	Chefs database is encrypted with a 128-bit AES content key in CBC mode	Re-encryption schemes that realize a stronger notion of security, and the usefulness of proxy re- encryption method of adding access control to a secure file system	In this only a limited amount of trust is placed in the proxy and proxy re-encryption to achieve CCA2 security in a multi-user setting
7.	Enabling Public Auditabilit y and Data Dynamics for Storage Security in Cloud Computing	Qian Wang Cong Wang	TPA-ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations	Third party auditor and merikle hash tree	Linux	Public auditability for storage correctness assurance.	Do not address the issue of data privacy

8.	Provable Data Possession at Untrusted Stores	Giuseppe Ateniese Randal Burns	Weaker guarantee by enforcing storage complexity	Provable Data Possession (E- PDP)	Linux	The PDP model for remote data checking supports large datasets in widely distributed storage systems.overhe ad of server is low	It provide a weaker guarantee by enforcing storage complexity
9.	Privacy-Preserving Audit and Extraction of Digital Contents	Mehul A. Shah Ram Swaminat han	Privacy preserving auditing and extraction of digital contents	Encrypted Key Extraction using Modified version	Java	Protocols are privacy-preserving, in that never reveal the data contents to the auditor	There are no fair and explicit mechanisms for making the services accountable for data loss
10.	PORs: Proofs of Retrievabili ty for Large Files	Bedford Hopkinton	Cryptographic proof of knowledge (POK), donot verify that archives do not delete or modify files prior to retrieval	Proof of retrivability method	Java	The goal of a POR is to accomplish the checks without users having to download the filesthemselves and quality- of-service guarantees	This imposes some computational overhead beyond that of simple encryption or hashingas well as larger storage requirements on the prover

Table 1: Comparison of security schemes

4. CONCLUSION

The paper covers the essential security loop holes as well as security requirements of an existing Cloud system. A generalized view of these issues have been presented here to enhance the importance of understanding the security flaws of the Cloud computing framework and devising suitable countermeasures for them. Finally, various cloud security schemes have been discussed on a comparative framework. On a whole, the paper aims at constructing a proper snapshot of the present scenario and future prospects of Cloud security.

5. REFERENCES

[1] Song, Dawn Xiaoding, David Wagner, and Adrian Perrig. “Practical techniques for searches on encrypted data.” In Security and Privacy, Proceedings. pp. 44-55. IEEE, 2000.
[2] Goldreich, Oded, and Rafail Ostrovsky. “Software protection and simulation on oblivious RAMs.” Journal of the ACM (JACM) 43, no. 3 (1996): 431-473. .
[3] Goh, Eu-Jin. “Secure indexes.” IACR Cryptology ePrint Archive 2003 (2003): 216.
[4] Chang, Yan-Cheng, and Michael Mitzenmacher. “Privacy preserving keyword searches on remote encrypted data.” In International Conference on Applied Cryptography and Network Security, pp. 442-455. Springer Berlin Heidelberg, 2005.
[5] Kamara, Seny, and Kristin Lauter. “Cryptographic cloud storage.” In International Conference on Financial Cryptography and Data Security, pp. 136-149. Springer Berlin Heidelberg, 2010..
[6] Boneh, Dan, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. “Public key encryption with keyword search.” In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 506-522. Springer Berlin Heidelberg, 2004.
[7] Maniatis, Petros, Mema Roussopoulos, Ed Swierk, Kevin Lai, Guido Appenzeller, Xinhua Zhao, and Mary Baker. “The mobile people architecture.” ACM SIGMOBILE Mobile Computing and Communications Review 3, no. 3 (1999): 36-42.
[8] Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, and Srinivasan D. 2008. TVDc: managing security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev. 42, 1 (January 2008), 40-47.
[9] Wu H, Ding Y, Winer C and Yao L, "Network security for virtual machine in cloud computing," 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, 2010, pp. 18-21.
[10] Wang Q, Wang C, Li J, Ren K, and Lou W. 2009. Enabling public verifiability and data dynamics for storage security in cloud computing. In Proceedings of the 14th European conference on Research in computer security (ESORICS'09), Michael Backes and Peng Ning (Eds.). Springer-Verlag, Berlin, Heidelberg, 355-370.
[11] Kazi Z & S.V V. (2017). Security Attacks and Solutions in Clouds.
[12] Hashizume K, Rosado D.G, Fernández-Medina E, and Fernandez E.B, “An analysis of security issues for cloud computing”, J. Int.Serv. App. pp. 1-13, vol. 4(5), 2013.
[13] Sen J, "Security and privacy issues in cloud computing", Architectures and Protocols for Secure Information Technology Infrastructures, pp.1- 45, 2013..
[14] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, “Hey, you get off my cloud: Exploring information leakage in third party compute clouds,” CCS’09, Proceedings of the 16th ACM conference. On Computer and Communications Security, pp. 199-212, ACM New York, NY, USA, 2009. ISBN: 978-1-60558-894-0.
[15] L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009. DOI: 10.1109/ICWS.2009.144.
[16] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010. DOI: 10.1109/MITP.2009.89.
[17] “Amazon ec2 sip brute force attacks on rise”,http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/.