OVERVIEW OF SECURITY ISSUES IN CLOUD COMPUTING

K. Arumugam[1], P. Sumathi[2]

[1]*Research Scholar/Department Of Computer Science, Government Arts College, Coimbatore (India)*

[2]*Assistant Professor/Department Of Computer Science, Government Arts College Coimbatore (India)*

ABSTRACT

Cloud computing is an ambiguous weapon from the privacy and security perspectives. Regardless of its likely to provide a low cost security, organizations may increase hazards by storing delicate data in the cloud. A comprehensive study of cloud computing security and privacy concerns are provided in this work. Security is one of the major issues which hamper the growth of cloud. Also the various security and privacy enhancement methods that are evaluated in the previous works have been analysed and discussed. This would serve as the promising analysis to know about the strengthening approach used for resolving the privacy issues and the security threats occurred in the cloud resources. In this paper, several Cloud computing system providers about their concerns on security and privacy issues are analysed.

Keywords: Cloud Computing, Enhancement Methods, Privacy Issues, Security Policies, Virtualization.

I. INTRODUCTION

Cloud computing does not have a common accepted definition yet. The National Institute of Standards and Technology (NIST) defined [9] cloud computing is described as a dynamic and often easily extended platform to provide transparent virtualized resources to users through the Internet. Cloud computing architecture consists of three layers are Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS). Although each service model has security mechanism but security needs also depends upon where these services are located, in private, public, hybrid or community cloud. The clouds are also viewed as five component architectures that comprise clients, applications, platforms, infrastructure and servers.

- Public clouds in which the physical structure is owned and accomplished by the service provider.
- Private clouds in which the structure is owned and accomplished by a specific organization.
- Hybrid clouds which include permutations of the previous three models.
- Cloud deployment models collected with their internal structure (IaaS, PaaS, SaaS).

1.1 Key Points To Cloud Security Alliance Model

- IaaS is the furthermost level of service with PaaS and SaaS next two above elevations of service.
- Moving up each of the service inherits abilities and security apprehensions of the model beneath.
- IaaS provides the structure, PaaS provides platform development environment and SaaS delivers operating background.

- IaaS has the minimum level of combined functionalities and combined security while SaaS has the most.

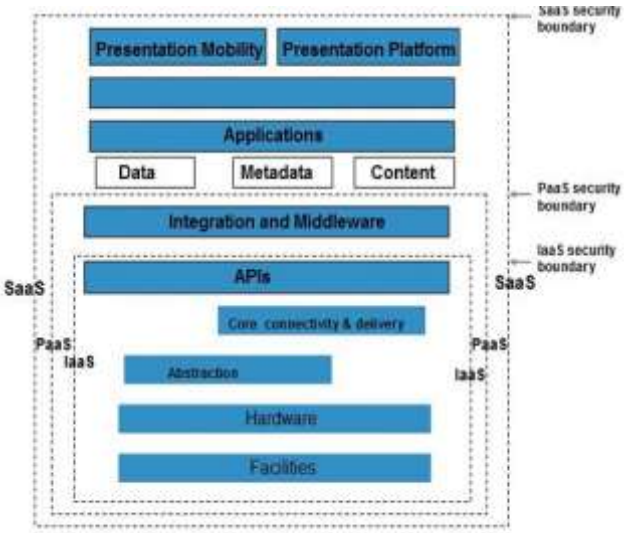

Fig .1: Cloud Security Alliance Model

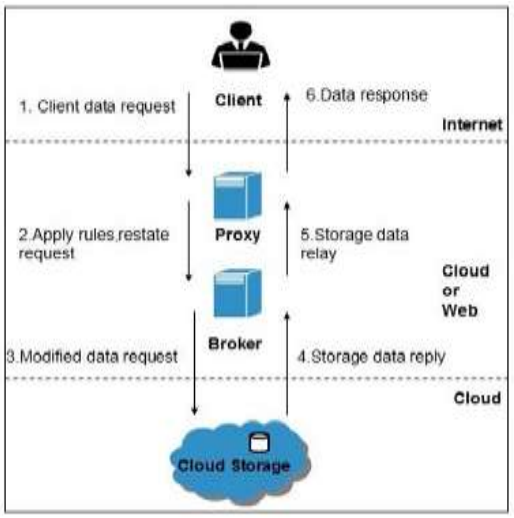

Fig.2: Brokered Cloud Storage Access System

1.2 Types Of Security Challenges In The Cloud

The main contribution [5] of the cloud provides a holistic study of the security issues in the clouds that cover almost all the cloud components (datacentres, computing infrastructure, interfacing and networking, etc.), network layers (application, transportation, IP, etc.), and cloud stakeholders (providers, consumers, third party contractors, etc.). Cloud provides a comprehensive survey on the cloud security and privacy concerns that includes:

- Cloud computing security issues (vulnerabilities, threats, and attacks)
- Attack taxonomies
- Relations and addictions among attacks
- Recognised attacks
- Proportional analysis of some of well-known countermeasures
- Understandings from the current security explanations to identify and address unattended security tasks.

II. RELATED WORKS

In this Survey, comparative contrivances and the systems which are engaged prior to attain a security and privacy are discoursed. And also the advantages and disadvantages of each technique are discoursed. Affording to the survey of the earlier contrivance, it finds that the current system executed has more advantages. C. Wang, Q. Wang, K. Ren, and W. Lou, focuses [7],[8] on the ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centres. In this work effective and flexible distributed scheme with two salient features, opposing to its predecessors is proposed in order to ensure the correctness of the user behaviour. Thus the result of this work

shows that it is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, focuses [10],[13] on verifying the authenticity of data has emerged as a critical issue in storing data on untrusted servers. It arises in peer-to-peer storage systems, network file systems, long-term archives, web-service object stores, and database systems. Such systems prevent storage servers from misrepresenting or modifying data by providing authenticity checks when accessing data. In this work two provable secure data possession (PDP) is proposed which allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. Thus the result of this work shows that it offer a probabilistic possession guarantee by sampling the server's storage, make it practical to verify possession of large data sets. Previous schemes that do not allow sampling are not practical when PDP is used to prove possession of large amounts of data. J. Yuan and S. Yu, defines [14] due to a number of unprecedented advantages resource elasticity, on-demand self-service, location independent resource polling, cloud storage is increasingly attracting customers including both organizations and individuals. Currently, millions of users have been using cloud storage services including Amazon S3, Microsoft Skydrive, Google Cloud Storage, iCloud, and Dropbox. In this work the first POR scheme with public verifiability and constant communication cost proposed. In this proposed scheme, the message exchanged between the prover and verifier is composed of a constant number of group elements; different from existing private POR constructions, our scheme allows public verification and releases the data owners from the burden of staying online. Thus the result of this work shows that PCPOR scheme achieves constant communication size, efficient computation performance as well as low storage overhead. More than this by supporting the public verifiability, this scheme releases the data owner from onerous verification tasks, which need to be centralized to the data owner in previous private POR scheme with constant communication size. B. Wang, B. Li, and H. Li, proposed [4], in a cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost. In this work Knox, a privacy-preserving auditing mechanism is proposed for data stored in the cloud and shared among a large number of users in a group to maintain the data integrity. In knox advantage of group signatures is considered to construct homomorphic authenticators, so that the third party auditor is able to verify the integrity of shared data without retrieving the entire data, but cannot reveal the identities of signers on all blocks in shared data. Thus the result of this work shows that Knox has a better performance when auditing data shared among a large number of users. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, [11],[12] evaluated an outsourcing of data essentially means that the data owner (client) moves its data to a third-party provider (server) which is supposed to – presumably for a fee – faithfully store the data and make it available to the owner (and perhaps others) on demand. The main issues of outsourced data are how to frequently, efficiently and securely verify that a storage server is faithfully storing its client's (potentially very large) outsourced data. In this work highly efficient and provably secure PDP technique based entirely on symmetric key cryptography is proposed, while not requiring any bulk encryption to address the issues of outsourced data. Thus the result of this work shows that compared to the POR scheme, proposed work provides better performance on the client side, requires much less storage space, and uses less bandwidth. Bo Chen, Reza Curtmola, Giuseppe Ateniese and Randal Burns, [2] proposed a technique of remote data checking (RDC) has been shown to be a valuable technique by which a client (acting as a verifier) can efficiently establish that data stored at an untrusted server

remains intact over time. This kind of assurance is essential to ensure long term reliability of data outsourced at data centers or at cloud storage providers. In this work RDC-NC, a novel secure and efficient RDC scheme for network coding-based distributed storage systems. RDC-NC mitigates new attacks that stem from the underlying principle of network coding. Thus the result of this work shows that RDC-NC scheme can be used to ensure data remains intact when faced with data corruption, replay, and pollution attacks. The performance evaluation shows that RDC-NC is inexpensive for both clients and servers. B.Wang, B. Li, and H. Li, [3] defines about the cloud offers data storage services with much lower prices than the cost of maintaining data on personal devices, people tend to outsource the hosting of their data to the cloud. By enjoying such storage services in the cloud, data owners are able to freely access their outsourced data on different devices and locations, and easily share their data with others. In this work certificateless public auditing mechanism is proposed to eliminate the security risks introduced by the public key infrastructure (PKI). Thus the result of this work shows that a public verifier is not only able to audit data integrity in the cloud but also able to eliminate possible security risks introduced by PKI in previous solutions. It proves that the security of proposed mechanism is based on the CDH assumption and DL assumption. Experimental results show that proposed mechanism is efficient. Ari Juels and Burton S. Kaliski Jr, [1], introduces the trends are opening up computing systems to new forms of outsourcing, that is, delegation of computing services to outside entities. Improving network bandwidth and reliability are reducing user reliance on local resources. Energy and labor costs as well as computing-system complexity are militating toward the centralized administration of hardware. In this work a proof of Retrievability (POR) scheme is proposed which may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file (or bit string) F. The goal of a POR is to accomplish these checks without users having to download the files themselves. Thus the result of this work shows that POR reduces the users burden is to accomplish these checks (delete or modify files) without users having to download the files themselves. A POR can also provide quality-of-service guarantees, i.e., show that a file is retrievable within a certain time bound. C Henry, H. Chen and Patrick P. C. Lee, focused [6] on cloud storage offers an on-demand data outsourcing service model, and is gaining popularity due to its elasticity and low maintenance cost. However, security concerns arise when data storage is outsourced to third-party cloud storage providers. In this work data integrity protection (DIP) scheme for a specific regenerating code is proposed, while preserving the intrinsic properties of fault tolerance and repair traffic saving. DIP scheme is designed under a Byzantine adversarial model, and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. Thus the result of this work shows that or Upload, which is a regular operation in archival storage, the DIP encoding part contributes up to about 40% of the running time with our default parameters. For the monetary cost, the overhead mainly comes from AECC, which expands our stored data by roughly n0/k0 times. In particular, we preserve the data transfer cost of NC Cloud during repair, which is the most significant M Khaba, M.Santhanalakshmi, defines [15] about the cloud computing that is a virtualized resource where we want to store all our data with security measurement so that some application and software can get full benefits using this technology without any local hard disk and server for our data storage. In this work an effective and flexible Batch Audit scheme with dynamic data is proposed to reduce the computation overheads. To ensure the correctness of user's data the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud. Thus the result of this work shows that proposed scheme is highly efficient and provably secure. From this protection for cloud data, user can be strong belief for his uploaded data for any future purpose or his any other related process

without worry. All the works discussed above clearly show the different methodologies used to provide a privacy and security prevention for the cloud data users as well as for cloud data owners. All of the above discussed technologies are meant to be solved various types of security threats and also possible ways to provide privacy.

TABLE.1: Summary Of The Topics Considered In Each Approach.

S. No	TITLE	AUTHOR	METHOD	ADVANTAGES	DISADVANTAGES
1	Ensuring Data Storage Security in Cloud Computing	C.Wang,Q.Wang, K.Ren, and W. Lou	Computing architecture	Effective and flexible distributed scheme	Colluding attacks
2	Provable Data Possession at Untrusted Stores	G. Ateniese, R. Burns, R.Curtmola, J.Herring, L.Kissner,Z. Peterson, and D. Song	Probabilistic possession guarantee	To prove possession of large amounts of data	Do not allow sampling
3	Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud.	J. Yuan and S. Yu	POR scheme	The data owner from onerous verification tasks	Low storage overhead
4	Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud	B. Wang, B. Li, and H. Li	Knox	Construct homomorphic authenticators	Knox is not affected by the number of users
5	Scalable and Efficient Provable Data Possession	G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik	Secure PDP technique	Symmetric key cryptography is proposed	Potentially very large
6	Remote Data Checking for Network Coding-based Distributed Storage Systems	Bo Chen, Reza Curtmola, Giuseppe Ateniese, Randal Burns	RDC scheme	Novel secure and efficient	Intact over time
7	Certificate less Public Auditing for Data Integrity in the Cloud	B.Wang, B. Li, and H. Li	Certificate less public auditing mechanism	To eliminate possible security risks	Maintaining data on personal devices
8	PORs: Proofs of Retrievability for Large Files	Ari Juels and Burton S. Kaliski Jr	Proof of Retrieve ability scheme	Quality-of-service guarantees	Computing services to outside entities
9	Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage.	Henry C. H. Chen and Patrick P. C. Lee	Data integrity protection (DIP) scheme	Fault tolerance and repair traffic saving	Third-party cloud storage providers
10	Remote Data Integrity Checking in Cloud Computing	Khaba M.V, M.Santhanalakshmi	Flexible Batch Audit scheme	Highly efficient and provably secure	Without any local hard disk and server for our data storage

III. CONCLUSION

Security and privacy enhancement methods that are evaluated in the previous works have been analysed and discussed. This would serve as the promising analysis to know about the strengthening approach used for resolving the privacy issues and the security threats occurred in the cloud resources. In this paper, we investigate several Cloud Computing system providers about their concerns on security and privacy issues. The detailed explanation of these techniques is briefed and also summarizes the advantages with parameters of the different techniques in cloud computing environment. Various types of possible ways to overcome these issues are discussed and different types of cryptographic mechanisms that are used to resolve the security threats are analysed. At the end of this survey, effective cryptographic mechanism is proposed to provide the effective prevention from the security attacks as well as better privacy preservation for the data owners and data consumers.

REFERENCES

[1] A Juels and B. S. Kaliski, PORs: Proofs of Retrievability for Large Files, In the Proceedings of ACM CCS 2007, 584–597.

[2] B Chen, R. Curtmola, G. Ateniese and R.Burns, Remote data checking for network coding-based distributed storage systems, In the Proceedings of the ACM workshop on Cloud computing, 2010.

[3] B Wang, B. Li, H. Li, Certificateless public auditing for data integrity in the cloud, In the Conference of IEEE on communications and Network Security (CNS), October-2013, 136-144.

[4] B Wang, B. Li, and H. Li, Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud in the Proceedings of ACNS, Springer-Verlag, June 2012, 507–525.

[5] Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing, 2009, http://www.cloudsecurityalliance.org.

[6] C Henry, H. Chen and Patrick P. C. Lee, Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage, In the Proceedings of SRDS, 2012.

[7] C Wang, Q. Wang, K. Ren, and W. Lou, Ensuring data storage security in cloud computing, In the Proceedings of IWQoS, Charleston, USA, 2009.

[8] C Wang, Q. Wang, K. Ren, and W. Lou, Towards secure cloud data storage, In the Proceedings of IEEE GLOBECOM on March-2009.

[9] Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/cloud- 102511.cfm (Accessed on 25 August 2013).

[10] G Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, Provable Data Possession at Untrusted Stores, In the Proceedings of CCS, 2007, 598–609.

[11] G Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, Scalable and Efficient Provable Data Possession, Proceedings of SecureCommunications, 2009, 1–10,

[12] G Ateniese, S. Kamara, and J. Katz, Proofs of storage from homomorphic identification protocols, In ASIACRYPT, 2009, 319–333.

[13] H Wang, Proxy Provable Data Possession in Public Clouds, In the IEEE Transactions on services computing, Volume-6, No-4, October-December, 2013.

[14] J Yuan and S. Yu, Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud Computing, Hangzhou, China, May-8, 2013.

[15] M Khaba and M.Santhanalakshmi, Remote Data Integrity Checking in Cloud Computing, International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), Volume: 1 Issue: 6, June-2013, 553–557.