A Survey on Security Services In Cloud Computing

S. Muthakshi M.Sc., M.Phil., [#1], Dr. T.Meyyappan M.Sc., MBA. M.Phil., Ph.d., [*2]

# Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu,India.

Abstract— **Cloud Computing has brought an incredible change in operations of the IT industries. The cloud computing has benefited the IT industries with less infrastructure investment and maintenance. As cloud provides services like Infrastructure-as-service (IaaS), Platform-as-Service (PaaS) and Software-as-service (SaaS) to its clients, it is essential that it also ensures data security to its clients. Security is an essential service to be provided exclusively in public cloud and hybrid cloud environment where in the data can be easily hacked or tampered. This paper aims to provide a comprehensive review on the essentiality of Security- as- Service in cloud computing scenario. The paper also presents the significance of data security and the various existing security techniques for the cloud.**

Keywords— ***Data integrity, outsourced data, Third Party Auditor (TPA), Audit Protocol Blocker (APB), cloud server provider (CSP), cloud user, Reed Solomon code (RS), error localization..***

I. INTRODUCTION

Cloud storage offers huge amounts of storage space and resources to the cloud users. Due to this the users depend on the providers in order to access their data stored in the cloud storage. The outsourced data is vulnerable to various internal and external threats which challenge the data integrity. To achieve the assurance of data integrity efficient methods of correctness verifications are to be carried out on behalf of the cloud users. The proposed system provides the verification of cloud storage and correctness with the Third Party Auditing. The internet-based online services provide various computing resources and huge amounts of storage space. However this trend is eliminating the need for local machines to handle and maintain the user's data. Due to this platform shift the users depend on their cloud service providers for the availability and integrity of the stored data. The cloud infrastructures are being more powerful and reliable than personal computing devices, yet there are number of internal and external threats for the integrity of data stored in cloud server. As the user don't have the local copy of outsourced data, the cloud service providers can behave unfaithfully to them regarding the status of their outsourced data. Outsourcing data into the cloud helps in reducing the cost and complexities of maintaining the data, but there is no strong assurance of data integrity and availability for both enterprise and individual cloud users. In order to achieve the assurances of cloud data integrity and availability methods that enable on-demand data correctness verification has to be done on behalf of cloud users. The data stored in the cloud database may not only be accessed but also be frequently updated by the users that which includes insertion, deletion, modification, and appending. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging. Last but not the least, the deployment of cloud computing is powered by data centers running in a simultaneous, cooperated, and distributed manner. In the file preparation to provide redundancies and guarantee the data dependability against Byzantine server's Reed Solomon erasure correcting code is used, where a storage server may fail in arbitrary ways. By utilizing the unique verification key with erasure-coded data, whenever data corruption has been detected during the storage correctness verification the identification of the misbehaving servers can be done. In order to save the time, computation resources, and the online burden of users, we also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to TPA and can be worry-free to use the cloud storage services.

II. RELATED WORK

Kui Ren [7], proposed the publicly auditable cloud data storage which is able to help the cloud economy become fully established. This auditing service helps the data owners' to maintain their data effectively that is present in the cloud storage. The proposed system accounts the users regarding the usage of their data by both the user himself and the TPA. Services for the legacy users is made available, who may not only access but also modify the data in the cloud.

Qian Wang [9], proposed a system that deals with the problem of ensuring the integrity of data storage in cloud with the help of a Third Party Auditor. Data integrity is achieved through the public auditing that is carried out on the users data by the Third Party Auditor. Block tag authentication is made to handle the data from the cloud storage efficiently. For the data that is stored in the cloud database, there is need for remote data integrity check which assurers the cloud users with a sense of security regarding their data. The third party audit ting has to be made available in such a way that no additional burden is introduced to the cloud users. A single Third Party Auditor is capable of handling multiple auditing tasks, which is achieved with the bilinear aggregate signature technique.

Cong Wang [6], proposed an auditing system which is carried out in such a way that the Third Party Auditor does its job without demanding the copy of user's data. Also the Third Party Auditor is not capable of deriving the user's data while performing the auditing task. To verify the correctness of the cloud data on demand from the cloud users the Third Party Auditor is used, who without retrieving a copy of the whole data or introducing additional online burden to the cloud users performs the auditing.

Mehul A. Shah [5], proposed a system that describes approaches and system hooks that support both internal and external auditing of online storage services. Online service oriented economy is which businesses and end users purchase IT services from a variety of online service providers. Third-party auditing is an accepted method for establishing trust between two parties with potentially different incentives. Auditors assess and expose risk, enabling customers to choose rationally between competing services.

III. SECURITY ISSUES ENCOUNTERED IN CLOUD COMPUTING

A guaranteed security service will enhance the business performance of the cloud service provider. Security is an essential service to be provided to the clients, a cloud service provider should assure. Secure cloud is a reliable source of information. Protecting the cloud is a very important task for security professionals who are in charge of the cloud. Cloud can be protected by protecting the data, making sure data is available for the customers, delivering high performance for the customers, using Intrusion Detection System on cloud and to monitor any malicious activities. For the safety purpose, the provider's must provide a support system for the client's so that every client must be able to recover their own data loss in the cloud environment. Therefore, the encryption technique must be adopted in cloud by the provider's to their client's for integrity and authentication of data.

When it comes to Security, cloud has lot of difficulties. The provider's must make sure that the client does not face any problem such as data loss or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user and there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. The various problems faced by the cloud computing can be classified as:

1. Data protection:

To be considered protected, data from one customer must be properly segregated from that of another; it must be stored securely when "at rest" and it must be able to move securely from one location to another. Cloud providers have systems in place to prevent data leaks or access by third parties. Proper separation of duties should ensure that auditing or monitoring cannot be defeated, even by privileged users at the cloud provider.

2. Authentication:

The authentication of the respondent device or devices like IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some "unfixable flaws" such as "trusted machine" status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered. One way to avoid IP spoofing by using encrypted protocols wherever possible. They also suggest avoiding ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged.

3. Data Verification:

Things like tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups. Resource isolation ensures security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache.

4. Infected Application:

Vendor should have the complete access to the server for monitoring and maintenance, thus preventing any malicious user from uploading any infected application onto the cloud which will severely affect the customer. Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures (application-level firewalls) be in place in the production environment

5. Availability:

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

IV. SECURITY METHODS

A. Authenticating cloud users and Third Party Auditor using verification key

The user and Third Party Auditor must be authenticated in order to use the services provided by the cloud service provider. Once the users or the Third Party Auditor has successfully completed the registration process, the verification code is sent to the mail id provided during the registration time. The cloud service provider decides the fate of the cloud user and the TPA. On the confirmation by the CSP the users will receive a conformation mail regarding their services.

Now the users can login into the cloud server in order to request the service form the cloud server. Each and every time the user or the TPA tries to access their account a verification key is generated to authenticate them. This verification key is generated by using the time and date function which can be used to provide maximum security.

Verification key that is generated is unique and so it can be generated only once for that particular time when the user or the Third Party Auditor is login to use the cloud service. This verification code is used to grant access to the user and the Third Party Auditor.

B. File distribution to the cloud storage

After successful login the cloud user can carry on the file operations that are granted by the CSP. In cloud data storage, we rely on erasure-correcting code to distribute the data file across a set of servers. Reed-Solomon erasure-correcting code is used to create redundancy parity vectors from data vectors in such a way that the original data vectors can be reconstructed from data and parity vectors. By placing each of the vectors on a different server, the original data file can survive the failure on the server without any data loss. The encoded file is obtained by multiplying the data file and the dispersal matrix, derived from a Vander monde matrix.

C. Correctness verification and error localization

Localization of the error is a potential way to eliminate errors in storage systems. It is also of critical importance to identify potential threats from external attacks. However, many previous schemes do not explicitly consider the problem of data error localization. The proposed scheme integrates the correctness verification and error localization i.e., misbehaving server identification with the help of the auditing results provided by the TPA along with the distributed erasure correcting code. The user verifies whether the received values remain a valid codeword determined by the secret matrix. The inconsistency among the storage is successfully detected by using the audit reports, the erasure codes are used to further determine where the potential data error lies in

.

D. Third Party Auditor

As discussed, in case the user does not have the time, feasibility, or resources to perform the storage correctness verification, they can optionally delegate this task to an independent third-party auditor, making the cloud storage publicly verifiable. However, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy. The TPA should not learn user's data content through the delegated data auditing. If the blinding of data vector is done before file distribution encoding, the storage verification task can be successfully delegated to third party auditing in a privacy-preserving manner. The correctness validation and misbehaving server identification for TPA is enhanced with the usage of the Audit Protocol Blocker. There is no way for TPA to learn the data content information during auditing process as the APB monitors the entire transaction.

E. Audit Protocol Blocker

The proposed system incorporates the previous system advantages and extends to find the unauthorized user, to prevent the unauthorized data access for preserving data integrity. The proposed system monitors the user requests according the user specified parameters and it checks the parameters for the new and existing users.

The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the audit protocol otherwise the system automatically blocks the audit protocol for specific user. If the TPA tries to read the user's content at the time of auditing the APB comes into light and blocks the appropriate TPA form granted accesses. This remains the same for the authorized users also.

V. EVALUATION

Ref No	**Context of Research**	**Problem Discussed**	**Research Type**
1	Service delivery models survey in Cloud Computing	Different Security risks that pose a threat to the cloud.	Theoretical study
2	Security in Enterprise Cloud	Security Techniques for applications in cloud	Theoretical study
3	Web Security issues in cloud computing.	Cloud Security problems	Theoretical study
4	Research Issues in Cloud Computing	Security Challenge, Data Challenges Performance Challenges	Theoretical study
5	Study of Security Issues in Cloud Computing	Security Issue mainly faced in the Industry.	Theoretical study

6	The Potential of Homeomorphic Encryption in cloud	Security issues affecting and proposed homomorphism encryption.	Theoretical study
7	Challenges and Security Issues in Cloud Computing	Focusing on the types of Cloud Computing and service service deliveries.	Theoretical study

VI. CONCLUSION

In this study different security issues research papers were studied briefly. In both larger and smaller scale organizations they are using cloud computing environment because of large advantage of cloud computing. The cloud computing has different security issues in threats in user view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. The bond between service providers and users is necessary for providing better cloud security.

In this paper we analyse the security issues, threats and challenges in wide acceptance of cloud computing, because there may be loss of data and privacy. Researchers Scholars and IT security professionals must press forward towards practical achievements in security and privacy to users. Our study identifies top security concerns of cloud computing, these concerns are security risks, techniques, problems, challenges and security issues of cloud computing and its methods.

VII. REFERENCES

[1]. S. Subashini and V. Kavitha ,A survey on security issues in service delivery models of cloud computing., *Journal of Network and Computer Applications, Vol. 34, No. 1*, Jul, 2010

[2]. Chang-Lung Tsai and Uei-Chin Li, Information Security of Cloud Computing for Enterprises, *Advances on Information Sciences and Service Sciences. Vol. 3, No. 1,* pp. 132-142, Feb 2011

[3]. Danish Jamil, Hassan Zaki, Security Issues In Cloud Computing And Countermeasures, *International Journal of Engineering Science and Technology, Vol. 3 No. 4,* pp. 2672-2676, April 2011

[4]. V. Krishna Reddy, B. Thirumala Rao, Dr. L.S.S. Reddy and P. Sai Kiran , Research Issues in Cloud Computing, *Global Journal of Computer Science and Technology, Vol. 11 No. 11* July 2011

[5]. Krishna Chaitanya.Y, Bhavani Shankar.Y, Kali Rama Krishna.V andV Srinivasa Rao, Study of security issues in Cloud Computing, *International Journal of Computer Science and Technology ,Vol. 2, No. 3,* Sept 2011

[6]. Aderemi A. Atayero, Oluwaseyi Feyisetan , Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption, *Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 10*, October 2011

[7]. Kuyoro S. O, Ibikunle.F and Awodele O, Challenges and Security Issues in Cloud Computing *International Journal of Computer Networks, Vol. 3, No. 5*, pp. 247-255, 2011