Volume 2, Issue 1, January 2015 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Privacy Preservation Techniques in Cloud Computing- A Review

Deepika Gour
Research Scholar
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:deepika.gour.1990@gmail.com

Prof. Raghvendra Singh Tomar
Assistant Professor
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: raghvendra_tomar@rediffmail.com

Prof. Ankur Pandey
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P), [India]
Email :- ankur.pandey1205@gmail.com

Dr. Mukta Bhatele
Head of Department
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

ABSTRACT

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. But during the access of data security is an important issue that needs to be maintained during communication. Since various protocols are implemented for the security of these cloud data Storage. Here an efficient technique is implemented using the hybrid combination of Access Policy based Elliptic Curve based Encryption. The proposed methodology provides a secure and dynamic auditing protocol for the secure access of the cloud data storage. In this paper we are presenting a survey of privacy preservation in cloud storage. We also discuss various method proposed by various researchers.

Keywords:— *Privacy preservation, Public verifiability, cloud storage, hybrid cloud.*

I. INTRODUCTION

With growing Internet scenario cloud computing is novel technique to serve better and secure services. Recently e-business is progressively more conducted over the Internet. Cloud computing is the hottest emerging computing technology where data storage, platform, and IT services are offered over the internet. Due to immense availability of resources and numerous tasks being submitted to the task management becomes important for optimal scheduling which affects the efficiency of the whole cloud computing environment. The use of Cloud Computing is ahead reputation due to its mobility and massive availability in minimum cost. The Cloud Computing provides its users benefit of extraordinary access to expensive data that can be turned into valuable insight that can help them achieve their business objectives.

Preventing the cloud from involving in ranking and entrusting all the work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead precludes information security. The issue of secure multi keyword top-k retrieval over encrypted cloud data, thus, is: How to make the cloud does more work during the process of retrieval without information leakage [1]. Clouds can be explained as pools of virtualized resources that can be easily used and accessed. For optimum resource utilization

the resources in cloud can be reconfigured dynamically. With the help of strong cloud architectures its mass computing and storage centers organizations and individuals are benefited while utilizing them. Cloud computing basically contains virtualization, on -demand deployment, Internet delivery of services, open source software etc. [2].

With the help of internet and central remote servers cloud computing maintains data and applications. Cloud computing helps the consumers and businesses to use clouds applications and resources without installing and accessing the personal files on any computer through internet. Cloud Computing provides efficient computing by centralizing storage, memory, processing and bandwidth promising lower costs, rapid scaling, easier maintenance, service availability. The main focus needs upon the data security and privacy. Services provided by cloud computing are [3].

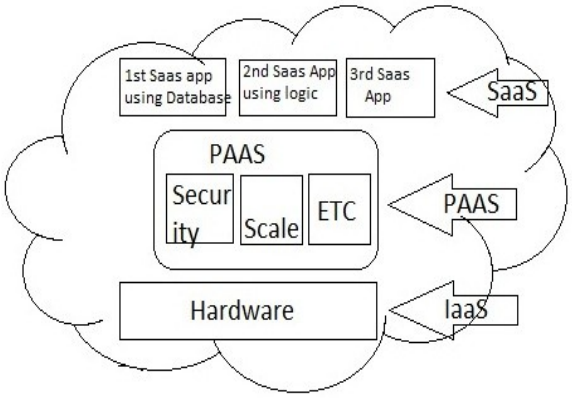

Figure 1. Cloud Computing Services

Cloud computing provides computing, storage, and networking as services rather than products. It allows the user to shift work and resources from their personal computers or even individual enterprise applications to a set of cloud computers. Cloud Computing solves the problems of hardware, machine failures etc. The advantage of cloud computing is its elasticity property which is the ability to add capacity or applications at the same moment without any prior notice and the pay-as-you-go approach enables the small and medium sized enterprises to use elasticity property as the vendor has many customers the per-unit cost to each customer can be lowered. Larger companies manage collaborations easily in the cloud [4].

Efficient cloud computing can be capable to manage different data centers. These data centers are able to run diverse workload with time just because of running virtual machines (VMs) inside them. This will lead high and low recourse utilization. To deal with this problem enhanced virtualization mechanism were developed and recent researches still going on in this era [5]. Cloud computing has been visualized as the next generation information technology (IT). It is especially constructed for enterprises to offer extraordinary advantages like; location sovereign resource pooling, ubiquitous network access, on-demand self-service, usage -based pricing, transference of risk and rapid resource elasticity [6].

Cloud security refers to the security of data, networking and other resources from viruses, worms, hackers, intruders etc. as far as security issues are concerned its is of two types: first one is category of cloud service providers while another one is users of it. Various points should be discovered that says that how secure cloud services are achieved? Some common parameter that are essential for cloud securities are: authentication, privacy, personal and physical security, availability and application security. Security plays a vital during the transmission of data from the sender to the receiver in any environment. The cloud computing provides on demand self service methodology that authorizes users to request resources dynamically as a best benefit. Data can be stored and retrieved remotely and due to this conventional cryptographic algorithm is not used for security. Once the data has been stored on cloud data storage security should be maintained by cloud service provider. To

maintain data security, publicly auditable cloud storage providers trusted third party auditor (TPA) to verify the data integrity of sourced data to ensure security [7].

To ensure cloud data storage security, TPA calculates the service quality from an objective and autonomous perspective. Public audit capability also permits clients to delegate the integrity verification tasks to TPA in case they are not being able to commit necessary computation resources performing continuous verifications [8]. The privacy-preserving public auditing is uniquely integrating the homomorphic non-linear authenticator with random masking technique. The individual auditing of TPA can be tedious and very inefficient [9]. Within cloud environment, the clients themselves are unreliable or cannot afford the overhead of performing frequent truthfulness verifies. Therefore, for realistic use, it seems more balanced to equip the verification protocol with public verifiability that is predictable to play a more significant role in achieving economies of scale for Cloud Computing [10]. Verifiability is kind of authentication mechanism. This will used to authenticate or validate the party or sometimes used to authenticate TPA. Verifiability of two types private Verifiability and public Verifiability. Private Verifiability is more secure. Public Verifiability is forced user to do not upload private data in cloud storage and stored data should be correctly stored [11].

II. Related Work

Patel, Chandrakant D., Shah, Amip J., "Cost Model for Planning, Development, and Operation of a Data Center,"[12] for the first-time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). Thorough analysis shows that our proposed solution enjoys "as-strong-as -possible" security guarantee compared to previous SSE schemes, while correctly realizing the goal of ranked keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution.

Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"[13], we propose a secure cloud storage system supporting privacy-preserving public auditing. Our work is among the first few ones to support privacy-preserving public auditing in cloud computing, with a focus on data storage. Besides, with the prevalence of cloud computing, a foreseeable increase of auditing tasks from different users may be delegated to TPA. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably

secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," [14], we present such a system—Cloud Capacity Manager (CCM)—an on-demand compute capacity management system and its methods for dynamically multiplexing the compute capacity of virtualized data centers at scales of that combines various low-overhead techniques, motivated by practical on-field observations, to achieve scalable capacity allocation for thousands of machines. CCM achieves this scale by employing three-level hierarchical management architecture. CCM also sheds light on the tradeoffs due to two unavoidable issues in large-scale commodity data centers: 1) maintaining low operational overhead, given variable cost of performing management operations necessary to allocate resources, and 2) coping with the increased incidences of these operations' failures. The capacity managers at each level continuously monitor and aggregate black-box VM CPU and memory usage information, and then use this aggregated data to make independent and localized capacity allocation decisions. An experimental evaluation on a fairly large infrastructure, that to achieve better capacity multiplexing, the focus needs to not only be on the accurate prediction of workload demand and aggressive optimization of the allocation algorithms, but also on dealing with the practical limitations of real-life infrastructures.

Cong Wang et al [15] propose a privacy-preserving public auditing system for data storage security in cloud computing. They utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process that not only removes the burden of cloud user from the tedious and possibly expensive auditing task, although also assuages the users' fear of their outsourced data escape. Taking into consideration TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, they further extend our privacy-preserving public auditing protocol into a multiuser situation, where the TPA can execute numerous auditing tasks in a batch manner for better efficiency [15].

To accomplish privacy-preserving public auditing, they suggest to uniquely integrating the homomorphic linear authenticator with random masking method. In this protocol, the linear combination of sampled blocks in the server's reaction is masked with randomness generated by the server. With random masking, the TPA no longer has all the essential information to construct up a accurate group of linear equations and for that reason cannot derive the user's data content, no issue how many linear combinations of the identical set of file blocks can be composed. Alternatively, the rightness corroboration of the block-authenticator pairs can still be accepted in a new way even with the occurrence of the randomness. Their design makes employ of a public key-based HLA, to provide the auditing protocol with public auditability [15].

By integrating the HLA with random masking, this protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server (CS) during the efficient auditing procedure. The algebraic and aggregation properties of the authenticator further benefit of this design for the batch

auditing. This public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. This scheme enables an external auditor to audit user's cloud data without learning the data content. This also supports scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner [15].

They consider a cloud data storage service involving three various entities, as shown in figure 2: the user who has big amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources the third-party auditor that has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon demand. Users are dependent on the CS for cloud data storage and preservation. They may also vigorously work together with the CS to access and update their stored data for various application intentions. As users no longer possess their data in the neighborhood, it is of critical importance for users to ensure that their data are being correctly stored and maintained. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, whereas hoping to keep their data confidential from TPA [15].

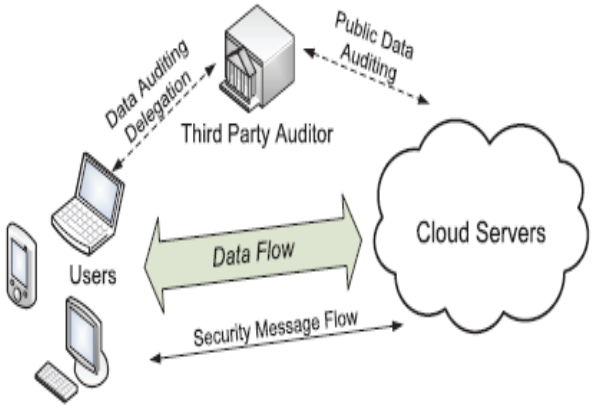

Figure 2: The architecture of cloud data storage service.

M.A. Shah et al [16] proposed solution to offer storage service accountability is throughout independent, third party auditing and arbitration. The customer and service enter into an agreement or contract for storing data in which the service provides some type of payment for data loss or failing to return the data intact, e.g. free prints, refunds, or insurance. In such a contract, the two parties have contradictory incentives. The service provider, whose objective is to make a profit and preserve a reputation, has an incentive to hide data loss. On the other hand, customers are terribly untrustworthy, e.g. casual home users. Customers can innocently or fraudulently claim loss to get paid. Thus, they engage an independent, third party to arbitrate and confirm whether stored and retrieved data is intact. This protocol has three important operations, initialization, audit, and extraction. For audits, the auditor interacts with the service to check that the stored data is intact. For extraction, the auditor interacts with the service and customer to check that the data is intact and return it to the customer [16].

This protocol shift the burden of maintenance these secret keys to a storage service. Since services are already in the business of maintaining customers' data and privacy, the keys are safer with them. Keeping the data content confidential from the service is

discretionary. A customer can keep the keys and encrypted data with the same service, thereby enlightening the contents to that service and allowing it to offer value-added features away from storage like search. Otherwise, the customer can separate the keys and encrypted data onto non-colluding services to maintain complete privacy. The auditor is responsible for auditing and extracting both the encrypted data and the secret keys. Although they present the protocols for handling the encrypted data for wholeness, they are straightforward extensions of existing techniques. They also describe methods for privacy preserving auditing and extraction of digital contents. These schemes separate the data into two pieces, an encryption key and the encrypted data. This protocols consent to an auditor, with minimal long-term state, to audit both those pieces and extracts those pieces without revealing the fundamental contents of either. Using this protocol, all these properties can be achieved without requiring the customer to maintain any long-term state. The protocols for the encrypted data rely on cryptographic hashes and symmetric key encryption [16].

3. CONCLUSION

Cloud computing enables various users to share or access resources over internet, but during the data sharing or storage in cloud security plays a vital role and hence various auditing protocols are implemented for the security of these cloud data and also provides privacy preservation between users. In this paper, some of the privacy preservation and public audits are addressed and the techniques to overcome them are surveyed. While some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy.

REFERENCES:

[1] Yu, Jiadi, Peng Lu, Yanmin Zhu, Guangtao Xue, and Minglu Li. "Towards Secure Multi-Keyword Top -k Retrieval over Encrypted Cloud Data," *IEEE transactions on dependable and secure computing*, vol. 10, no. 4, pp. 239- 250, July/ August 2013.

[2] Pankaj Arora, Rubal Chaudhry Wadhawan and Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service", *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277-128X, vol. 2, issue 1, Jan. 2012.

[3] Song, Dawn, Elaine Shi, Ian Fischer, and Umesh Shankar. "Cloud data protection for the masses", *In IEEE Computer*, vol. 45, no. 1, pp. 39-45, 2012.

[4] Priya, P. Shanmuga, and R. Sugumar. "Multi Keyword Searching Techniques over Encrypted Cloud Data", *International Journal of Science and Research (IJSR)*, ISSN: 2319-7064, vol. 3, issue 3, pp. 410 - 412, March 2014.

[5] Kesavan, Mukil, Irfan Ahmad, Orran Krieger, Ravi Soundararajan, Ada Gavrilovska, and Karsten Schwan "Practical Compute Capacity Management for Virtualized Datacenters", *IEEE Transactions On Cloud Computing*, Vol. 1, No. 1, pp. 88 – 100, 2013.

[6] P. Mell and T. Grance, "The NIST definition of cloud Computing", *Special Publication 800-145*, 2012.

[7] Swathi Sambangi "Cloud Data Storage Services Considering Public Audit for Security", *Global Journal of Computer Science and Technology Cloud and Distributed*, ISSN: 0975-

4172, Vol. 13, Issue 1, pp. 1 – 6, 2013.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.

[9] Srinivas, D. "Privacy-Preserving Public Auditing In Cloud Storage Security." *International Journal of computer science and Information Technologies*, ISSN: 0975-9646, vol. 2, no. 6, pp. 2691-2693, 2011.

[10] Zhu, Yan, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, and Stephen S. Yau. "Efficient provable data possession for hybrid clouds." *In Proceedings of the 17th ACM conference on Computer and communications security*, pp. 756-758. ACM, 2010.

[11] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" *Proceedings of the 14th European conference on Research in computer security (ESORICS'09)*, pp. 355-370, 2009.

[12] Patel, Chandrakant D., Shah, Amip J., "Cost Model for Planning, Development, and Operation of a Data Center," Internet Systems and Storage Laboratory, HP Laboratories, Palo Alto, June 9, 2005.

[13] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[15] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, pp. 362 – 375, February 2013.

[16] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", 2009 Proceedings of the 14th European conference on Research in computer security (ESORICS'09), pp. 355-370, 2009.

* * * * *