Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.509 – 513

SURVEY ARTICLE

A Survey on Security in Cloud Computing

Varsha Yadav[1], Preeti Aggarwaal[2]

[1]PG Student, Department of Computer Science Engineering, Maharshi Dayanand University, Rohtak, India

[2]Assistant Professor, Department of Computer Science Engineering, Maharshi Dayanand University, Rohtak, India

[1] vrshyadav91@gmail.com; [2] preetaggarwal@gmail.com

Abstract—*Cloud computing is an emerging technology in IT industry. In Cloud computing technology, computing resources are provided as a service over the internet, rather than a product. Cloud computing has gained great attention from the industry but there are still many issues that are hampering the growth of cloud. One of these issues is security of data stored on the servers of cloud service providers. This paper presents a survey on various security schemes that provide data security in cloud computing.*

Keywords—*Cloud computing; security; data storage; encryption algorithms; data partitioning scheme*

I. INTRODUCTION

Cloud computing is a model which allows the user to use services provided by Service provider on pay per use bases. In Cloud computing the computing services are delivered over the Internet. The Cloud services provide the individuals and businesses with the opportunity to use software and hardware that are managed by third parties at remote locations. Cloud computing model provides convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In cloud computing there are three service models (Iaas, Paas and SaaS) and four deployment models i.e. public, private, community and hybrid cloud are available, which are explained below. Since data is stored in the data centers, the security of data is an important issue. This paper present a survey of various security schemes which helps in ensuring security of data stored centers of the cloud.

A. Cloud Service Models

The major cloud computing service models are known as software as a service, platform as a service, and infrastructure as a service

1) Software as a Service (SaaS): In Software as a Service, consumer has the capability to use the provider's applications running on a cloud infrastructure. The client can access the applications from various devices, through a thin client interface, such as a web browser (e.g. web-based e-mail). The consumer need not to manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

2) Platform as a Service (PaaS): In Platform as a Service, consumer is provided with the capability to deploy onto the cloud infrastructure consumer created or acquired applications, produced using programming languages ,libraries, services and tools supported by the provider. The consumer does not has the responsibility to manage or control the underlying cloud

infrastructure including network, servers, operating systems, or storage, but he needs to have control over the deployed applications and possibly application hosting environment configurations.

3) Infrastructure as a Service (IaaS): In Infrastructure as a Service consumer has the capability to provision processing, storage, networks, and other fundamental computing resources, and is allowed to deploy and run arbitrary software, which can include operating systems and applications. The consumer need not to manage or control the underlying cloud infrastructure but he has the responsibility to have control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

B. Deployment Models

In cloud computing four types of clouds are available which are public, private, community and hybrid cloud.

1) Public Cloud: In public clouds, the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are less secured and more vulnerable than private clouds [1].

2) Private Cloud: Unlike public clouds, in the Private Clouds [1], the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control. However they require the company to still purchase and maintain all the software and infrastructure.

3) Community Cloud: The community cloud is defined as the cloud infrastructure which is shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party.

4) Hybrid Cloud: It is the type of cloud which forms from the combination any two (or all) of the three models discussed above.

Cloud computing is an emerging technology in IT sector. It ha gained great attention from the industry. Since the data is stored in the data centers of the cloud, the security of data is an important issue. This paper present a survey of various security schemes which helps in ensuring security of data stored centers of the cloud.

II. LITERATURE REVIEW

Cloud Computing is the delivery of computing and storage capacity as a service but there is lack of confidence in trusting, because user's data are processes remotely in unknown servers. To overcome this problem [2] provides an object-centered technique to extend owners' full control over his own data. In particular, a logging mechanism is provided for user's data and ensures that any access to their data will trigger authentication which is used to protect user's data and also monitor the actual usage of data in the cloud. Distributed auditing mechanism is also described in this paper.

Various security issues and some of their solution are explained in [3]. This paper concentrates mainly on public cloud security issues and their solutions. Data should always be encrypted when stored (using separate symmetric encryption keys) and transmitted. If this is implemented appropriately, even if another tenant can access the data, all that will appear is gibberish. So a method is proposed such that the whole data is encrypted along with the cryptographic key.

In [4] author has given a brief introduction on Cloud computing and touched some of the security issues related to a cloud. Having explained the problems in the cloud, author has also proposed some solutions to the same with the help of algorithms like the DES and RAS Algorithms.

Cloud computing [5] in today's world is making wide differences between it and other technologies. The critical data of users can be stolen by various means whereas cloud computing is still not a secure way to store users data. This paper tries provides a review of what are various types of digital watermarking techniques and in what way the integrity of watermarking can be attacked so as throttle the system. The collaboration of digital watermarking when used for cloud computing can significantly result to make the system robust as well as secure user's data.

A brief introduction of cloud computing its types and security issue and approaches to secure the data in the cloud environment are described in [1].

In [6] a model is proposed for cloud storage and auditing using digital signature. TPA (Third Party Auditor) checks the integrity of data on the cloud on the behalf of the users, and hence TPA has full access of user's data. In this paper RSA algorithm is used for encryption and decryption which follows the process of digital signature for the message authentication. First the user and the TPA generates their own private key and public key with respect to the strong RSA algorithm. The public keys have been shared between them as the part of SLA or in some other ways. Then with respect to the protocol the message is encrypted and after that data is signed with the user's private key then the cipher is again encrypted with the TPA's public key. This package is now sent to the Cloud and also the TPA .The TPA now decrypts the encrypted message with his private

key and then de-signs the cipher with the user's public key to recognize the data. Then the same process of decryption is carried out in the cloud by the TPA to verify the correctness by comparing the data which he has with the stored one.

Increasing demand for cloud applications [7] has led to an ever growing need for security mechanisms. The most serious concerns are the possibility of lack of confidentiality, integrity and authentication among the cloud users and service providers. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication. In this paper symmetric and asymmetric cryptographic algorithms are adopted for the optimization of data security in cloud computing.

The cloud computing platform [8] gives people the opportunity for sharing resources, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. In this paper new security architecture is proposed for cloud computing platform. This ensures secure communication system and hiding information from others. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features, e.g. PaaS, SaaS and IaaS. This model also includes onetime password system for user authentication process. This research work mainly deals with the security system of the whole cloud computing platform.

Security issues and requirements in the Cloud and possible solutions of some the problems are discussed in [9]. An architecture model is developed for cloud computing to solve the data availability and error correction problem.

In [10] the problem of ensuring the integrity of data storage in Cloud Computing is studied. In particular, they have considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. The authors first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, they improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they further explore the technique of bilinear aggregate signature to extend the main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

With the advent of the World Wide Web [11] and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. This data would be more useful to cooperating organizations if they were able to share their data. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. In this paper these issues are addressed by combining cloud computing technologies such as Hive and Hadoop with XACML policy based security mechanisms that provide fine-grained access to resources. This paper further presents a web-based application that uses this combination and allows collaborating organizations to securely store and retrieve large amounts of data.

A k-out-of-n recursive information hiding scheme based on an n-ary tree data structure is described in [12]. In recursive hiding of information, the user encodes additional information in the shares of the secret intended to be originally shared without an expansion in the size of the latter. The described scheme has applications in secure distributed storage and information dispersal protocols. It may be used as a steganographic channel to transmit hidden information, which may be used for authentication and verification of shares and the reconstructed secret itself.

The scheme proposed in [13] is introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

A recursive computational multi secret sharing technique is presented in [14] that hides k - 2 secrets of size b each into n shares of a single secret S of size b, such that any k of the n shares suffice to recreate the secret S as well as all the hidden secrets. This may act as a steganographic channel to transmit hidden information or used for authentication and verification of shares and the secret itself. Further, such a recursive technique may be used as a computational secret sharing technique that has potential applications in secure and reliable storage of information on the Web, in sensor networks and information dispersal schemes. The presented technique, unlike previous computational techniques, does not require the use of any encryption key or storage of public information.

In [15] data partitioning scheme is used for implementing security. In this method data is first partitioned into two or more pieces and then the partitions are stored on randomly chosen servers on the network and the division of data is performed in such a way that the knowledge of all the pieces is required to recreate the data and that none of the individual pieces reveals any

useful information. Data reconstruction requires access to each server, login password and the knowledge of the servers on which the partitions are stored. This scheme may also be used for data security in sensor networks and internet voting protocols.This scheme does not perform encryption of the partitions. Several variations of this scheme are also described, which include the implicit storage of encryption keys rather than the data in which the data is encrypted and stored on single server and then the encryption key is partitioned and spread over the network, and where a subset of the partitions may be brought together to recreate the data.

In his well-known Information Dispersal Algorithm [16] paper, Rabin showed a way to distribute information in n pieces among n servers in such a way that recovery of the information is possible in the presence of up to t inactive servers. An enhanced mechanism to enable construction in the presence of malicious faults, which can intentionally modify their pieces of the information, was later presented by Krawczyk. Yet, these methods assume that the malicious faults occur only at reconstruction time. In this paper authors have addressed the more general problem of secure storage and retrieval of information (SSRI), and guarantee that also the process of storing the information is correct even when some of the servers fail. Our protocols achieve this while maintaining the (asymptotical) space optimality of the above methods. They also considered SSRI with the added requirement of confidentiality, by which no party except for the rightful owner of the information is able to learn anything about it. This is achieved through novel applications of cryptographic techniques, such as the distributed generation of receipts, distributed key management via threshold cryptography, and "blinding". An interesting byproduct of their scheme is the construction of a secret sharing scheme with shorter shares size in the amortized sense. An immediate practical application of their work is a system for the secure deposit of sensitive data. They also extend SSRI to a "proactive" setting, where an adversary may corrupt all the servers during the lifetime of the system, but only a fraction during any given time interval.

III. CONCLUSION

Cloud computing allows the users to store their information in the cloud, due to which users need not to worry about the space management for storing their large amount of information. Since the data is sored in the servers of data centers of cloud service providers, security of data is an important issue. This paper presents a survey on various methods that were proposed by the earlier researchers for enhancing the security of data stored on cloud.

IV. FUTURE WORK

Various methods that have been proposed by earlier researchers for enhancing the security of data stored in the cloud are explored in this paper. In future, we can propose a method in which data or information will be first partitioned into shares, these shares are then encrypted and also the key of fingerprint of the client will be attached with each share. These encrypted shares along with the key of the fingerprint will be stored on the server. This method will ensure the security of data stored in the servers of the cloud because, instead of storing the data on a single server, encrypted shares of data are stored on different servers, further the fingerprint's key of the sender are attached with each share and since fingerprints have zero collision property, only the original sender can retrieve the data.

REFERENCES

[1] S. Sharma, S. Soni and S. Sengar, "Security in cloud computing," National Conference on Security Issues in Network Technologies, Aug. 2012.
[2] K. Velammal and L. Sheela, "Secure data sharing in the cloud by maintaining integrity using logging mechanism," International Journal of Computer Science and Mobile Computing, Mar. 2014.
[3] G. Thomas, P.J.V. and P.Afsar, " Cloud computing security using encryption technique," IJASCSE, Oct. 2013.
[4] V. Alangar, "Cloud computing security and encryption," International Journal of Advance Research in Computer Science and Management Studies, Oct. 2013.
[5] N. Singh and S. Singh, "The amalgamation of digital watermarking and cloud watermarking for security enhancement in cloud computing," International Journal of Computer Science and Mobile Computing, Apr. 2013.
[6] K. Govinda, V. Gurunathaprasad and H. Sathishkumar, "Third party auditing for secure data storage in cloud through digital signature using RSA," International Journal Of Advanced Scientific and Technical Research, Aug. 2012.
[7] M. Sudha and M. Monica, "Enhanced security framework to ensure data security in cloud computing using cryptography, "Advances in Computer Science and its Applications, Mar. 2012.
[8] K. W. Nafi, T. S. Kar, S. A. Hoque and M. M. A. Hashem, " A newer user authentication, file encryption and distributed server based cloud computing security architecture," International Journal of Advanced Computer Science and Applications, 2012.

[9] A. Gupta, P. Pande, A. Qureshi and V. Sharma, "A proposed solution: data availability and error correction in cloud computing," International Journal of Computer Science and Security, 2011.
[10] Q. Wang C. Wang, K. Ren, W. Lou and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel And Distributed Systems,May 2011.
[11] V. Khadilkar, A. Gupta, M. Kantarcioglu, L. Khan and B. Thuraisingham, "Secure data storage and retrieval in the cloud," 6th International Conference on Collaborative Computing: Networking and Worksharing (CollaborateCom,), Oct. 2010.
[12] A. Parakh and S. Kak, "A tree based recursive information hiding scheme," in Proc. of IEEE ICC 2010 – Communication and Information System Security Symposium,2010.
[13] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Dec. 2010.
[14] A. Parakh and S. Kak, "Recursive secret sharing for distributed storage and information hiding," IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems,2009.
[15] A. Parakh and S. Kak, "Online data storage using implicit security," Information Sciences,2009.
[16] J. A. Garay, R. Gennaro, C. Jutla and T. Rabin, "Secure distributed storage and retrieval," Theoretical Computer Science,2000.

