A SURVEY ON USER PRIVACY PROTECTION METHODS IN CLOUD

Sharmila.J[1], Dhivyaa.C.R[2]

[1]*PG Scholar, Computer Science Engineering, Nandha college of Technology, Tamilnadu, India*

[2]*Assistant Professor, Computer Science Engineering, Nandha College of Technology, Tamilnadu, India*

Abstract- ***The increased use of cloud computing services has pressed the issue of privacy concerns of cloud services to the utmost importance. The cloud is open to all users and due to the openness, virtualization, various malicious service providers may exist in these cloud environments. Malicious service providers may attack the user's data and gain user's private data without their knowledge. The user are not aware of their privacy being at stake and still they use cloud services which becomes beneficial to the unauthorized service providers. This paper focuses on various privacy protection techniques that are provided in the enterprises to protect user privacy at both client side and server side. The methods deployed within each protection mechanisms are also analyzed.***

Keywords*: cloud computing, virtualization, cloud attacks, privacy protection*

1.INTRODUCTION

Cloud Computing is a type of outsourcing of services in Computer Science. Users can simply use it and they pay for what they consumed. As customersgenerally do not own the infrastructure or know all details about it, this becomes the main reason for attack on customer's data. In [1], a survey of intrusion detection techniques mentioned that use of virtualization technique in cloud infrastructure, integrated technologies and standard Internet protocols for running it. These may attract intruders, due to vulnerabilities involved in it. In [2], it is described that the hypervisor or monitor in virtual machine is an extra layer of softwarebetween an operating system and hardware platform that is used to operate multiple client virtual machines and is common to IaaS clouds. Besides virtualized resources, normally the hypervisor supports to conduct administrative operations in other application programming interfaces, like migrating,launching and terminating virtual machine instances. Compared with conventional, and the non-virtualized implementation, the addition of a hypervisor becomes a motivation in the attack surface. That is, there are application programming interfaces, sockets and input string, a hacker can use to cause damage to the system. Authorized Cloud users may pursuit to gain unauthorized privileges. In [1], some usual attacks are mentioned. The common attack is Insider attack, in which insiders may commit frauds and reveal information to others intentionally. This forms a serious trust issue. Another attack is flooding attack where attacker tries to flood victim by sending heavy load of packets from innocent host (zombies) in network. Flooding attack influence the service availability to the authorized user.

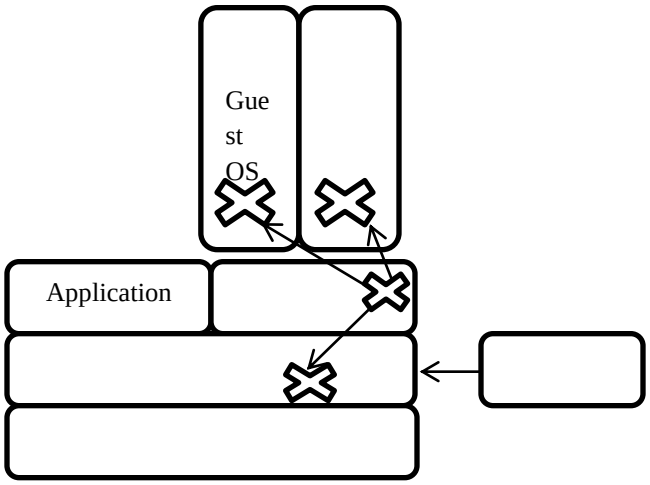

Fig – 1: Attack on Hypervisor through Host OS

Attacking a single server providing a certain service, an attacker can create a loss of availability on the intended service. This type of attack is called direct Denial of Service attack. Once the servers hardware resources are completely disabled by processing the bogus requests, then the other service illustration on the related hardware machine are no longer able to

perform their intended tasks. This type of distributed attack is known as indirect attack. Flooding attack may increase the usage bills remarkably as the Cloud is unable to determine among the normal usage and fake usage. Many such attacks are in common, this paper focus on preserving privacy of the cloud user. One such common solution is Firewall. Firewall protects the foremost entry points of system and is treated as the front defense line.

2. PRIVACY PROTECTION METHODS

Various methods have been put forward to overcome this issue of privacy preserving. This work studies some of those approaches and provides a concise outline. It is important, that the privacy has to be preserved anytime and anywhere. The protection can be done by both provider and user at server side and client side.

2.1 Encryption Strategies

The data can be encrypted and decrypted before storing in the cloud. User can encrypt their data while uploading it on the cloud and decrypt while downloading it. In [3], review of various encryption schemes is provided.

2.1.1 Key Policy Attribute Based Encryption

A set of descriptive attributes is labeled by the encryptor for each cipher text. An access structure is associated with Each private key that indicate which form of cipher-texts the key can decrypt. In the work of Jin sun [4], the key policy ABE is associated with the broadcast encryption to provide a dual system encryption. With this standard model, the scheme can achieve fixed-size public criterion, force no bound on attribute set size used for encryption.

2.1.2Cipher-text policy Attribute Based Encryption

Here attribute policies are associated with data and attributes are associated with keys. Decryption is possible only those keys which are collaborated with attributes satisfy the policy collaborated with the data. This encryption satisfies the security needs demanded by the customer.

2.1.3Cipher-text policy Attribute Set Based Encryption

A recursive set-based structure is framed by organizing user attributes and allows users to demand dynamic constraints on how those attributes may be associated to satisfy a policy.By using this techniquesencrypted data can be kept secret even if the storage server is not trustworthy; moreover, this method provide security against collusion attack. This methods are related to conventional access control methods such as Role-Based Access Control (RBAC).

2.1.4Fuzzy Identity-Based Encryption

As measured by the overlap distance metric, the identities a and a' should be close to each other then only it is possible to decrypt a cipher-text encrypted with an identity a' with a private key for an identity a. In fuzzy, a biometric can also be used as attributes for the identities.

2.2 IDENTITY BASED AUTHENTICATION

In [5], SSL Authentication Protocol is applied in cloud computing, will become so complicated that users will undergo a bulk point both in computation and communication. It based on the identity-based hierarchical model for cloud computing. In [6], the authors proposed a dynamic authentication protocol that can support dynamic operations in cloud. This enables only valid users to authenticate in cloud.

2.3 THIRD PARTY AUDITOR

Third party auditor checks the integrity of client data. The TPA checks the data integrity by the demand provided by the user and the audit reports help the user to examine the service risk. In [7], Wang proposed public auditing scheme which provides a*entire outsourcing* result of data not only the data itself, but also its integrity checking. It involves public auditability to allow TPA to verify the correctness of the cloud data and also ensure that there exists no cheating cloud server.

2.4 PROOF OF RETRIEVABILITY

A proof of retrievability (POR) is a solid proof by a file system (prover) to a client (verifier) that a target file F is flawless, in the sense that the client can fully recover it. In [8], qianwang proposed a Merkle hash tree technique to improve the proof of retrievability. A hash tree is a tree of hashes in which the leaves are data blocks hashes in, for instance, a file or set of files. Nodes added up in the tree are the hashes of their corresponding children.

2.5 DATA SELF DESTRUCTION

In [8], jinboxiang proposed the key-policy attribute-based encryption with time-specified attributes KP-TSABE to clarify some meaningful security problems by supporting user-defined authorization period and by providing fine-grained access control during the period. The hypersensitive data will be securely self-destructed after a user-specified expiration time. The KP-TSABE scheme is demonstrated to be secure under the decision l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) assumption.

2.6 INTRUSION DETECTION SYSTEM

In [9] ,it gives a new solution for preventing intruders from attacking. Regardless of company size or volume and magnitude of the cloud, this paper explains generated and injected into real customer service requests so that malicious service providers would not be able to characterize which requests are real ones if these requests how maneuver IT virtualization approach could be used to acknowledge a denial of service attack. A hypervisor has its own security sector, and it is the governing agent for everything within the virtualization host. Hypervisor can touch and affect entire operation of the virtual machines running within the virtualization host. There are numerous security sectors, but these security sectors remain within the same physical framework that, in a more conventional sense, only exists within a single security sector. This can motivate a security concern when an attacker takes control over the hypervisor. The attacker can choose this technology to perform an attack. Hence HIDS and NIDS are used.

2.7 ANONYMOUS ACCESS CONTROL

In [10], a new notion called k-times attribute-based anonymous access control is proposed, which is appropriately designed for backing cloud computing environment. With this new approach, a user can authenticate himself/herself to the cloud computing server namelessly. The server only knows the user need some required attributes, yet it does not know the identity of this user. Further, provided a k-times restriction for anonymous access control. That is, the server may restrict a appropriate set of users to access the system for a maximum k-times within a period or an event. Further additional access will be denied. It also prove the security of its instantiation.

2.8 NOISE INJECTION

In [11], Gaofeng Zhang proposed a time series pattern based noise generation technique for protecting the privacy of users. Noise obfuscation is an effective approach in this regard by utilizing noise data. For instance, noise service requests can be occurrence probabilities are about the same, and consequently related customer privacy can be protected. The probability fluctuation could not be covered by existing noise generation strategies, and it is a serious risk for the privacy of customer. To notify this probability inconsistency privacy risk, this paper efficiently develops a new time-series pattern situated noise generation technique for privacy protection on cloud.

3. CONCLUSION

Cloud providers need to defend the privacy and security of personal data that they hold on behalf of organizations and users. Although cloud computing has many advantages, there are still many actual problems that need to be solved. The various protection mechanisms are provided to overcome these problems are discussed. Thus, we need to develop privacy preserving strategy that overcomes the worries in privacy security and encourage users to adopt cloud storage services confidently.

REFERENCES

[1] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. &Rajarajan, M. (2013), "A survey of intrusion detection techniques in Cloud", in Journal of Network and Computer Applications", 36(1), pp. 42-57.doi: 10.1016/j.jnca.2012.05.003.

[2] Wayne Jansen., Timothy grance, "Guidelines on security and privacy in public cloud computing", in NIST special publication 800-144.

[3] Priyadarsini, K., ThirumalaiSelvan., "A Survey on Encryption Schemes for DataSharing in Cloud Computing", (IJCSITS), ISSN: 2249-9555 Vol. 2, No.5, October 2012.

[4] Jin Sun., Yupu Hu., Leyou Zhang., "A Key Policy Attribute Based Broadcast Encyption" in *The International Arab Journal of Information Technology, Vol. 10, No. 5, September 2013*

[5] Jaatun, M.G., Zhao, G., and Rong, C., "Identity-Based Authentication for Cloud Computing", (Eds.): CloudCom 2009, LNCS 5931, pp. 157–166, 2009.© Springer-Verlag Berlin Heidelberg 2009.

[6] Vishnu sekar. R., Nandhini. N., Bhanumathy. D., Hemalatha. M., "Identity based authentication for data stored in cloud", in international journal of Advanced research in Computer science and software engineering, vol 5, No.2, March 2015.

[7] Cong Wang., Qian Wang., KuiRen., "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, vol. 64, no. 5, may 2012.

[8] Qian Wang., Cong Wang., Jin Li1., Kui Ren1., and Wenjing Lou., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" in Proc. of ASI-ACRYPT'08. Springer-Verlag, 2008, pp. 90–107.

[9] JinboXiong., Ximeng Liu., "A Secure Data Self-Destructing Scheme in Cloud Computing" in IEEE transactions on cloud computing, vol. 2, no. 4, october-december 2014.

[10] AmanBakshi., yogesh, C., "Securing cloud from DDOS Attacks using Intrusion Detection System in virtual machine" in Proceedings of the 2004 IEEE International Conference on Advances in Intelligent Systems - Theory and Applications, 2004.

[11] Tsz Hon Yuen., Joseph K. Liu., Man Ho Au., XinyiHuang.,"k-Times Attribute-Based Anonymous Access Control for Cloud Computing" in IEEE transactions on computers, vol. 64, no. 9, september 2015.

[12] Gaofeng Zhang., Xiao Liu., Yun Yang.," time-series pattern based effective noisegeneration for privacy protection on cloud" in IEEE transactions on computers, vol. 64, no.5,may2015.

BIBILIOGRAPHIES

J.Sharmilareceived the B.E. degree in Computer science and Engineering from Nandha college of Technology in 2014. She is currently doing her M.E Computer science and Engineering in Nandha College of Technology, Erode,
India

C.R.Dhivyaa(ASP/CSE) working as Assistant Professor in Nandha College of Technology. She has published many national and international research papers. She has very depth knowledge of her research areas.