ISSN:0975-9646

Side Channel Security with Multiclouds

S. M. Bansode

Assistant Professor CSE department
SGGS Institute of Engineering and Technology
Nanded, Maharashtra

Abstract—cloud boon is on with security fear in minds. Cloud users are worried about attacks on the integrity, confidentiality and the availability of their important data in the cloud. Malicious cloud providers and other people could also pose side channel attacks. This paper focuses on side channel attacks in the cloud. It describes a Multi-clouds Distributed Instance (MCDI) model which is based on Multi-clouds service providers and its use to mitigate the side channel attack on the virtual instance of user.

I. INTRODUCTION

Cloud computing is a buzzword which offers dynamically scalable resources provisioned as a service over the Internet. It promises to reduce economical as well as operational expen-ditures for hardware and software.Clouds are categorized as public cloud which is offered by third-party service providers and involves resources outside the user's premises. The other type of cloud system is installed on the user's premise and is said to be private cloud. A hybrid approach is the combination of two public and private cloud. Services provided in any type of clouds are Infrastructure as a Service(Iaas), Platform as a Service(Paas), Software as a Service(SaaS) [l]. Cloud users may share the Infrastructure,Platform and Software. Thus sharing of resources pose security threats of confidentiality and integrity of data[2], [3], [5], [6].

Cloud owner and user have a many security issues and challenges. Security threats in cloud computing is presented in [5]. It discussed range of issues like attacks on cloud interfaces to misusing the cloud services for attacks on other systems. In the cloud computing paradigm user outsourcing sensitive as well as business-critical data and processes. Thus using a cloud service, the user given all data to the cloud provider have control over and not the user. Also using cloud for data-processing applications cloud (via IaaS or PaaS), a cloud provider gets full control on these processes. cloud user, needs to trust the cloud provider. An attacker who can get access to the cloud storage may take snapshots or change data in the storage. This might be done any time and number of times If an attacker has access to the processing functions of the cloud then attacker can modify these functions and its input and output data. Though it is assumed a cloud provider is honest and would provide the customer services without any interference in security of data but malicious employees of the cloud provider may compromise the security of data or processing logic. In [6], flaws and attacks on cloud infrastructures are discussed. Ristenpart et al. [7], [8] presented some attack techniques for the virtualization of the Amazon EC2 IaaS service. In their approach, the attacker allocates new virtual machines until one runs on the same physical machine as the victims machine. Then, the attacker can perform cross-VM sidechannel attacks to learn or modify the victims data.

The authors present strategies to reach the desired victim machine with a high probability, and show how to exploit this position for extracting confidential data, e.g., a cryptographic key, from the victims VM. Finally, they propose the usage of blinding techniques to fend cross-VM side-channel attacks. In [9], they discussed how interface of Amazons EC2 have security attack. Gruschka and Iacono [9] Shown Signature Wrapping Attack in the EC2 implementation.

Google Docs allows user to edit documents (e.g., text, spreadsheet, presentation) online and share these documents with other users. But this is an insecure system as if a document is shared with anyone, then this is accessible for everyone the document owner has ever shared documents with before. Thus unauthorized access to confidential data is possible. Thus cloud computing paradigm contains an implicit threat of working in a compromised cloud system. Thus if an attacker is able to get access to infiltrate the cloud system itself, all data and all processes of all users operating on that cloud system may become subject to malicious actions in an avalanche manner. Hence, the cloud computing paradigm requires an in-depth reconsideration on what security requirements might be affected by such an exploitation incident. For the common case of a single cloud provider hosting and processing all of its users data, an intrusion would immediately affect all security requirements: Accessibility, integrity, and confidentiality of data and processes may become violated, and further malicious actions may be performed on behalf of the cloud users identity. These cloud security issues and challenges triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Alongside with these security issues, the cloud paradigm comes with a new set of unique features that open the path toward novel security approaches, techniques, and architectures. Attackers could use side channels of cloud to steal the data[4].One promising concept makes use of multiple distinct clouds. Cloud providers should address security issues of user data. This paper proposes a new model Multi-clouds Distributed

Instance MCDI which uses Multi-cloud service providers instead of using single cloud and distributed instance.The purpose of the proposed new model MCDI is to address the risks challenges in cloud computing environment due to the side channel attacks.

II. MULTICLOUD ARCHITECTURES FOR SECURITY

Cloud providers are unable to fully assure security of data while it is stored or during processing and in transit. Bernstein and Celesti [8], [9] proposed approach of using multiple clouds. However, this work did not discuss security issues. Other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, and partly use cryptographic methods.

In [10] Jens-Matthias Bohli et. al. introduced a model of different architectural patterns for distributing resources to multiple cloud providers. This model is used to enhance the security benefits. In their model, they distinguish the following four architectural patterns for distributing resources to multiple cloud providers:

1. Replication of applications: An operation is carried out on more than one cloud and results from these clouds are compared. Thus user gets evidence on the integrity of the result.
2. Partition of application System into tiers:In this approach logic and the data are partitioned. This ensures protection against data leakage due to flaws in the application logic.
3. Partition of application logic into fragments: In this the application logic is divided and distributed to distinct clouds. There are two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider has the complete result of the operation. Thus, user will have data and application confidentiality.
4. Partition of application data into fragments: It allows data fragments to be divided into distinct clouds. Data confi-dentiality is maintained as none of the cloud providers gains access to all the data.

III. PROPOSED APPROACH

As discussed earlier Ristenpart et al. [4] presented side channel attack techniques for the virtualization of the Amazon EC2 IaaS service. The attacker runs virtual machines on the same physical machine as the victims machine and then perform cross-VM side- channel attacks to learn or modify the victims data. In this paper Partition of application logic into fragments approach to mitigate the side-channel attack on cloud is used. In this method the confidentiality of data and processing logic is secured. It tries to resolve the concern of a cloud user avoid fully revealing the data or processing logic to the cloud provider. The data should be protected while in the persistent storage, and also during the processing. In this architecture application logic needs to be partitioned into fine-grained parts and these parts are distributed to distinct clouds (see Fig. 1).

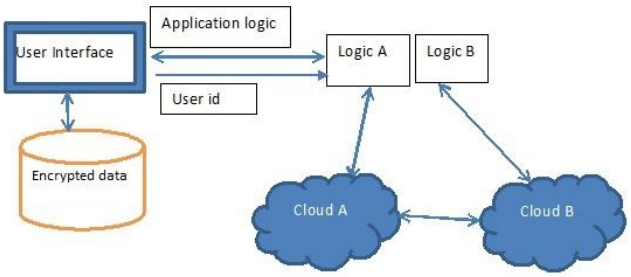

Fig. 1. The proposed approach: Partition of application logic with use of encrypted data

1) Obfuscating Splitting: In this approach, client application is divided and distributed to different clouds. Thus every single cloud has only some part of the application and gains only limited knowledge. Therefore, the method can hide parts of the application logic from the clouds. As discussed earlier Ristenpart [4] shown the side channel attacks on cache. The solution proposed in this paper to have the application logic divided and distributed over multiple clouds. Now consider an example where the victim user has an application which is to be processed on cloud. Victim user creates virtual machines on for example two clouds cloud A and cloud B from among multiple clouds. Victim partitions the application in part A and part B and sends the part of data which is needed there to process. These two virtual machines process the logic and return the results to victim user. Now suppose the attacker learns on which physical machine the victim has the virtual machine created then attacker would also create the instance on the same machine. Attacker may learn some data from this cloud which is incomplete information. Now attacker does not have the information regarding where the other instance of the victim is from among number of clouds. Thus the attackers goal of stealing the data from side channel attack would be defeated. In this method user nor victim has to partition application and send it over the clouds. This increases load on user. How to partition data is fully users view. Depending upon the application logic user may create the instance on more than on cloud. If the application logic needs to have the communication between the cloud they should interact with each other with a token of user id. Thus clouds can have the interaction as in the Fig 1. The question may arise about the partly stolen data. The attacker may steal some data from a cloud. The stolen data is not complete data but the attacker has succeeded partly which is not useful for the attacker. The proposed solution to the partly stolen data is Homomorphic ncryption.

2) Homomorphic Encryption: In Cloud computing scenario user may use encryption to the data.The processing logic and this encrypted data is sent to the Cloud provider. But this method requires to decrypt data at cloud provider to perform the operation. Thus client needs to provide the private key to the Cloud provider to decrypt data and perform required operations. This might affect the confidentiality and privacy of data which is stored in the Cloud.Homomorphic Encryption applied to Cloud Computing could be used to provide security.

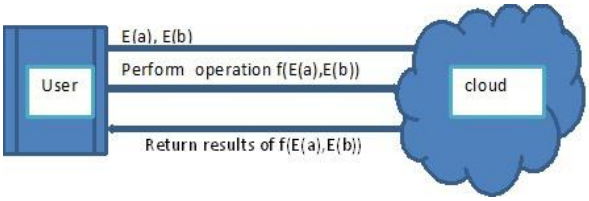

Fig. 2. Use of Homomorphic encryption in cloud computing

In Homomorphic encryption operation is performed on encrypted data without decrypting them as shown in Fig 2, and it produces the same results as if operations are worked directly on the original data. Thus user do not have to expose the data neither the secret key to the cloud provider.

For example if

- Ek is an encryption algorithm with key k.
- Dk is a decryption algorithm.

Dk (Ek (n)* Ek (m))= n*m OR Enc (x*y) = Enc(x)* Enc(y)
Dk (Ek (n)+ Ek (m))= n+m OR Enc (x+y) = Enc(x)+ Enc(y)

The first property is called additive homomorphic encryp-tion, and the second is multiplicative homomorphic encryption [11]. An algorithm is fully homomorphic if both properties are satisfied simultaneously. Security of cloud data can be ensured using Homomorphic encryption. This approach of encryption supports secure addition and multiplication of ciphertexts .

IV. CONCLUSION

In this paper Partition of application logic into fragments and homomorphic encryption approach is used to mitigate the side-channel attack on cloud. It suggests multiple cloud providers for gaining security and privacy benefits in cloud services. Use of multiple cloud and homomorphic encryption reduces the effect of stealing the data as the attacker could only extract part of data with much difficulty. Use of homomorphic encryption even reduces the retrieving of data by the attacker. Thus the goal of attacker has been distracted.

V. FUTURE SCOPE

This paper presented the technique to mitigate the side channel attack. The technique of multiple cloud with homo-morphic encryption is also useful for security and privacy for SaaS and Paas as well.

REFERENCES

[l] Michael Armbrust,Armando Fox,Rean Griffith,Anthony D. Joseph,Randy H. Katz,Andrew Konwinski,Gunho Lee,David A. Patterson,riel Rabkin-Ion Stoica, Matei Zaharia Above the Clouds: A Berkeley View of Cloud Computing Technical Report No. UCB/EECS-2009-28

[2] L. M. Kaufman, Data security in the world of cloud computing, IEEE Security and Privacy (2009), pp.61-64.

[3] Amandeep Verma and Sakshi Kaushal Cloud Computing Security Issues and Challenges:A Survey ACC 2011, Part IV, CCIS 193, pp. 445-454, 2011

[4] T. Ristenpart, E. Tromer, H. Shacham and S.Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,ACM, 2009, pp. 199-212.

[5] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2011), pp. 1-11.

[6] H. Takabi, J. B. D. Joshi and G. Ahn, Security and Privacy Challenges in Cloud Computing Environments, Security and Privacy, IEEE, 8 (2010),pp. 24-31.

[7] Mohammed A. AlZain, Ben Soh and Eric Pardede Department of Com-puter Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia. MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing

[8] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, Blueprint for the IntercloudProtocols and Formats for Cloud Computing Interoperability, Proc. Intl Conf. Internet and Web Applications and Services, pp. 328-336, 2009.

[9] Celesti, F. Tusa, M. Villari, and A. Puliafito, How to Enhance Cloud Architectures to Enable Cross-Federation, Proc. IEEE Third Intl Conf. Cloud Computing (CLOUD), pp. 337-345, 2010.

[10] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, IEEE, Luigi Lo Iacono, and Ninja Marnau Security and Privacy-Enhancing Multicloud Architectures IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[11] C. Gentry, A Fully Homomorphic Encryption Scheme, PhD dissertation, Stanford Univ., 2009