International Journal of Engineering & Technology, 7 (2.33) (2018) 513-514

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Keyless signature infrastructure solution for cloud attacks

Remya Chandran [1] *, Dr. A. Sasi Kumar [2]

[1] Ph.D. Research Scholar, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies(VELS VISTAS), Pallavaram, Chennai, India

[2] Professor, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies(VELS VISTAS), Pallavaram, Chennai, India

**Corresponding author E-mail: nivedika@gmail.com, askmca@yahoo.com*

Abstract

Keyless Signature Infrastructure (KSI) is a procedure that is used to distribute and verify the signature; only hash function cryptography is being used in this method. KSI uses block chain technology for the signing and verification of the signature. The paper will discuss the solution of different cloud attacks using Keyless Signature Infrastructure.

Keywords: *Cloud Attacks; Block Chain; Markle Tree.*

1. Introduction

To sign the data, a user communicates with the system (KSI) by submitting a hash-value of the data, the KSI will returned a signature that provides a secured cryptographic proof of the time of signature., source of origin, integrity of the signed data. The KSI signature is getting generated in Exabyte scale, the data is generated around the planet every second even though every data record will be signed using KSI with tiny computational, network overhead and storage. The signatures (KSI) are portable, it is becoming a part of the application, configuration files, responsible access, authentication and authorization assets etc.. Keyless signatures Infrastructure prevent different cloud attacks. KSI used to provide data integrity in cloud computing [4].

2. Different cloud attacks and KSI solution

2.1. Side channel attack

The attrackers targeting IaaS (Infrastructure as a Service Platforms) for side channel attacks. An attracker attempt to attack the cloud system by placing a virtual machine in the aimed cloud server system and then start a side channel attack. An IaaS model in cloud computing make available infrastructure like a collection of several computers, virtual machine(VMs) and storage location to store confidential and vital information, data documents etc.,

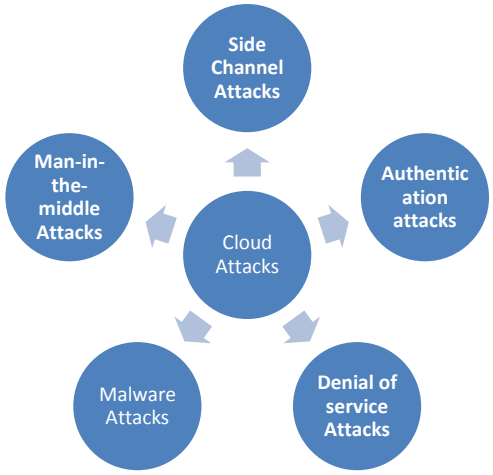


Fig. 1: Different Cloud Attacks.

2.1.1. KSI solution for side channel attack

Since the Merkle Signature Scheme is used in binary tree creation of KSI, It is challenging against all side channel attacks. In a differential side channel attack, the attacker snoop a side channel during the procedure of the signature to get the extra information. Since a new hash value is used for each signature, an attacker will not be able to collect information about a secret by matching the information obtained during the computation of two signatures. Because the secret values have no relation to each other. The Merkle Signature Scheme is public. All nodes can be published in a tree, because they all will be part of at least one signature and therefore will be public anyways.

2.2. Man-in-the-middle attack

This type of attacks happen when a communication established in two node or computer system. Usually the message content and message sequences are modified by the attackers. A man-in-the-

Copyright © 2018 Remya Chandran, Dr. A. Sasi Kumar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

middle attack allows a malicious actor to disrupt & send and receive data between the two users.

2.2.1. KSI solution for man-in-the-middle attacks

There was controversy about an attack on Whatsapp; the attackers execute the man in the Middle attack by pushing false keys. Whatsapp known as a very popular and secure messaging application, but unfortunately they unable to block the attack, The risk of false key transmission could be eradicate by publishing keys on a block chain and it will enable the application to verify the people whom you are communicating.

2.3. Denial of service attacks

The servers getting overloaded by Denial Of Service. The attackers send enormous number of request to the target servers to attack it. Hence it cannot process the additional requests.

2.3.1. KSI solution for denial of service attacks

Every gateway and aggregation server create regular upstream network traffic that won't depend the normal load, The customer will get isolated, and it will not allow to vital data loss about the actual service usage as well as arrange a reasonable denial of service attack protection[3].

2.4. Authentication attack

The cloud environment is easily attacked by this type of attacks; the authentication attacks allow the attacker to perform the attack very easily on servers. The attacker targets the followed user mechanism. The attacker's uses this mechanism for authentication captures and tries to access the confidential information. A different encryption and decryption mechanism used by attackers to transfer the data as very confidential. Before going to access the service, the service provider should store the key value and has to authorize.

2.4.1. Solution for authentication attacks

Since no key is used in Keyless Signature Infrastructure, Most of the authentication attacks can be prevented. Merkle Tree architecture is also used to prevent authentication attacks.

2.5. Malware injection attacks

Only based on the authentication and authorization the clients request is processed in the cloud computer environment, there is a chance of raw data's to take control over between the web server and web browser at the time of authentication, and an attacker can use this switch over time of metadata. The attacker uses this particular time and introduces a harmful code or a service to the cloud computing environment. This service or code will ditto to the service that is already in the cloud system. Once the code affected the cloud it will run continuously.

Table 1: Different Authentication Attacks

Authentication Attacks			
Cipher text Attack	Insider	Chosen-Plaintext Attack	Chosen-Cipher text Attack
Eavesdropping	Replay Attack	Password Discovery	Session Hijacking
Customer Fraud	Reflection	Known-Plaintext Attack	Shoulder Sniffing
Brute Force Attack	Dictionary Attack	Birthday attack	Network Sniffing

2.5.1. Solution for malware injection attacks

A real time verification code that has been generated by the real time signature verification ensure that only valid code is executed, this process block the attacker and not allowing to inject the malware code or service to the system or otherwise tamper with authorized set of instructions.

3. Conclusion

The keyless signature infrastructure (KSI) is used to provide integrity of data in cloud system, unlike other methods the keyless signature is not using keys for protecting the data and therefore it can overcome all the cloud related attacks that happened during the sharing of secret key, encryption and decryption process. KSI help the user to prevent all major attacks that is related with cloud computing. Even the KSI method can protect the attack against the Quantum computer that is going to get implemented.

References

[1] Raja,JabirMuhammed, Liza, SalamKanji,Huwida, Omar, "study of Different cloud computing attacks and countermeasures", International Conference on Advanced Communication Technology (ICACT) , ISBN 978-89-968650-7-0, 2016.

[2] Prachi,Satheesh,Sharma,"Security-Threats in cloud computing", Computing, Communication & Automation International Conference (ICCCA), July 2015.

[3] Akashdeep,Vinay,Subhramaniyam,Hanumath, "Solution to cloud DDoS attacks", IEEE July 2016.

[4] AhtoBudhas,Risto,Andres"KSI: Construct universal Distributed-Hash of Trees", International Association for Cryptologic Research(IACR) 2013.

[5] Jämthagen, Christopher, "On Offensive and Defensive Methods in Software Security" Published: 2016-10-19.

[6] S.Manikandasaran "Security- Attacks and Cryptographic Different Solutions for Stored Data in Cloud Public Storage", IRACST - International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555 Vol.6, Feb 2016.