Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secured Third Party Auditing in Cloud Computing

Vasantha V N Sainath
SITE, VIT University,
Vellore,India

K.Aravind
SITE, VIT University,
Vellore,India

Abstract— Cloud computing has grabbed the spotlight in the recent past and opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges.To address these security issues, a third party can be used as an auditor which in turn generally uses key based algorithms or cryptographic techniques to encrypt and protect the data. In this paper we propose a new technique called "Address authentication"to mitigate the main security threats like data protection, user authentication, data breach in cloud environment.

Keywords— Cloud computing, Third party auditor, Address authentication, Security, Side-channel attack

I. INTRODUCTION

During the recent past, Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. Committing to a cloud computing provider can result in significant cost savings and more streamlined, flexible operations. Enterprises that have adopted the cloud are finding that while cloud computing confers very real benefits, it also creates significant security challenges, which traditional network and perimeter security measures are inadequate to address. Organizations must protect their data, rather than their infrastructure, if they use the cloud at all.
Cloud computing security challenges fall into three broad categories:

Data Protection: This is one of biggest concerns with cloud computing since cloud data storage is that of data integrity and security at mistrusted servers. Critical security measures should be maintained since sensitive data is being placed in the hands of a third party.

User Authentication: User authentication is the second biggest challenge as data present on the cloud can be accessed any one. Data present in the cloud needs to be accessible only by those authorized to do so. In order to ensure the integrity of user authentication, Third Part Auditor (TPA) need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require.

Disaster and Data Breach: Another major challenge in cloud computing is contingency planning.TPA needs to tell the customers / companies how the data is being secured and what measures the service provider will be taking to ensure the integrity and availability of that data in case of an unexpected occur.Also what type of actions taken and alerts provided in case of a data breach.
CSA (Cloud Security Alliance) pointed to a research paper[8] from 2012 described how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other client's data as well. In side-channel attack the attacker extracts an ElGamal decryption key that was stored on a VM running the open-source GNU Privacy Guardusing the mostrecent version of the libgcrypt cryptographic library.This attack works every time when both attacker and target VMs were running on the same physical hardware.The attackerthen probes a given machine and minesall the cryptographic keys stored on it. In order to address these issues many schemes are proposed under different systems and security models [1], [2], [3], [4], [5].Most of the existing systems rely on encrypting the data and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. These encryption algorithms are mostly popular key generation encryption algorithms like RSA etc…which generates Public key – Private key or bilinear aggregate signature etc…for encryption [6], [7]. Since all the existing techniques are error prone and if the attackers have enough knowledge and experience in using these algorithms they can easily breach through these encryption techniques. So in this paper we propose a new model which is more secure and relatively easy to implement when compared to others.

II. PROPOSED ARCHITECTURE

The proposed architecture is an enhanced Third Party Auditor architecture in which the key generation algorithms used for "User Authentication" are replaced with our new technique called "Address Authentication".

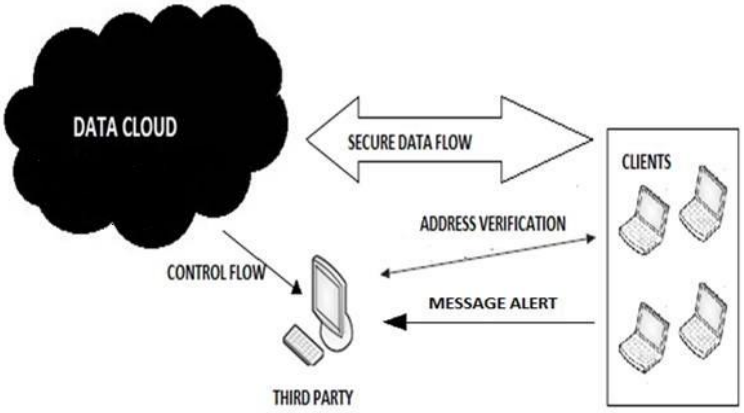

Fig 1: Secured TPA Architecture

The above diagram represents the architecture of the Secured Third Party auditing in which "Data cloud" is the CSP (Cloud Service Provider) where all the user / client data has been stored. The CSP's outsources the maintenance of the cloud to TPA's (Third Party Auditors) and the TPA will take care of all the user registrations and subscriptions to the cloud.

The data flow from Cloud to Client will be allowed only once the "Address" has been verified by the TPA thus providing "Data protection". Also an instant message alert will be triggered to the RMN(Registered Mobile Number) whenever there is an attempt for intrusion to prevent "Data Breach".

III. ADDRESS AUTHENTICATION TECHNIQUE

The proposed solution to the current security challenges in the cloud is securing the Third Party Auditing by using "Address authentication" technique which uses various combination of details combined as an "Address" to authenticate the user. Details include IP address / (MAC address + System Details) / Phone number as an additional key along with the normal profile credentials based on the device and location of the client from where the cloud data is being accessed.

Whenever there is an access request for the cloud data, the TPA cross checks the login credentials and "Address" based on the type of device being used to access the cloud and the location of the device, thus providing dual layer security against colluding attacks on cloud computing. The "Address Verification" is carried out based on the type of the device and location of the device from which the cloud data has to be accessed.

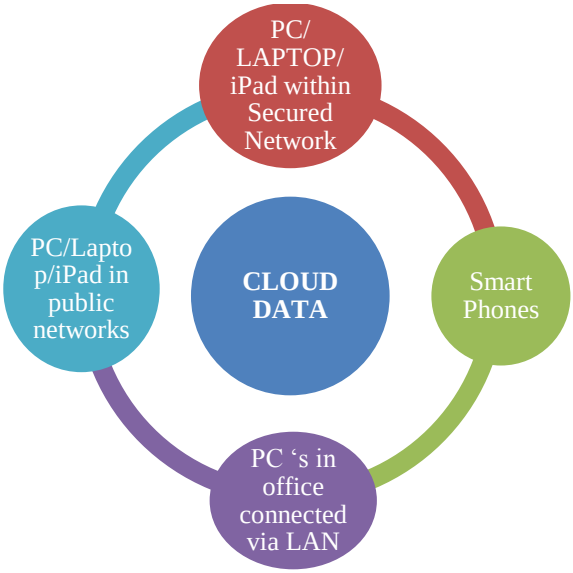

Fig 2: Locations + Device – Possibilities

Devices within Secured Network & PC's in office connected via LAN:

Most of the PaaS and IaaS client systems now –a- days are within a secured network i.e. all the PC's are connected to Ethernet switches with fixed LAN cables or connected to secured registered wireless routers.All the systems connected to this secured switches / routers have their MAC address registered with the switches / routers and are prevented from MAC address spoofing as all the system settings will be disabled by the administrator in the secured network and moreover there is MAC address locking in all the new switches / routers which will any way prevent the MAC address spoofing. So the IP addresses of the switches/routers are used as additional credentials in these scenarios's to grant the access to cloud data to the clients.

ADDRESS = IP address of the switches / routers

Any new device being added to these secured networks to access the cloud should be protected from MAC spoofing and the MAC address should be added to the router / switches MAC ID table. More over TPA should perform periodic audits of all the systems and switches settings to make it more secure.

Devices in public networks:

For the devices which are requesting access to cloud data via public networks such as from coffee shops / air ports / form private Wi-Fi hot spots, the MAC address +System Details is used as "Address" to grant the access to cloud data to the clients i.e. MAC address + Location of the device + Platform (OS which the device is using to access the cloud) +Browser (for web based cloud services) is used for authentication. This is the similar authentication technique as Facebook's "Remember Browser".

ADDRESS = MAC address + Location of the device + Platform +Browser

Whenever the device moves to a new location apart from the "Trusted Locations"(Registered while subscribing to cloud data), a random OTP(One time Password) will be sent to RMN(Registered Mobile number). Moreover the "Location expiry time" can also be set by user. (E.g. 1 hour for coffee shop, 3 hours for Airport etc…) where 7 days is the default expiry time. TPA should perform periodic maintain a log for all the actions done by user outside the secured network and audits should bedone periodically maintain data integrity.

Smart Phones (Either under Public / Secured Network):

For all the clients with registered mobile numbers restricted access i.e. read only access and only to non sensitive data can be provided when accessing the cloud data when accessing via smart phones using mobile number for authentication.

ADDRESS = Registered Mobile Number.

This is the similar authentication technique as how WhatsApp identifies its user's.

TPA should periodically cross verify the RMN to prevent data breaches.

In all the above mentioned cases, the Address along with normal login credentials is verified by the TPA before allowing the access to cloud data in order to ensure all the security concerns are met.

IV. REQUIREMENTS

The following are the three major requirements which TPA has to take care to provide secured cloud computing:

Maintaining logs and Periodic Auditing:TPA should maintain a log of all the cloud activities of all the users and also need to periodically audit the samein order to make the system more powerful and efficient which in turn results in efficient defect and intrusion tracking.

Address / Detail Gathering:KYC (Know your Customer)exercise should be conducted for all the existing clients to gather the required details such as IP, MAC addresses, System Details and Mobile numbers.

Address Validation: Background verification needs to be done to validate all the details before giving access to the cloud data to the client devices. This should be a repetitive process which should be done periodically to phase out the malicious / obsolete users from accessing the cloud data.

V. RESULTS

Security Analysis: In this section, we evaluate the security of the proposed scheme under the security model defined earlier. We have tried breaching into the cloud from various unauthorized devices which are not registered with the TPA and every time the STP (Secured Third Party) architecture system succefully declined the access request and also issued a mobile alert to RMN.

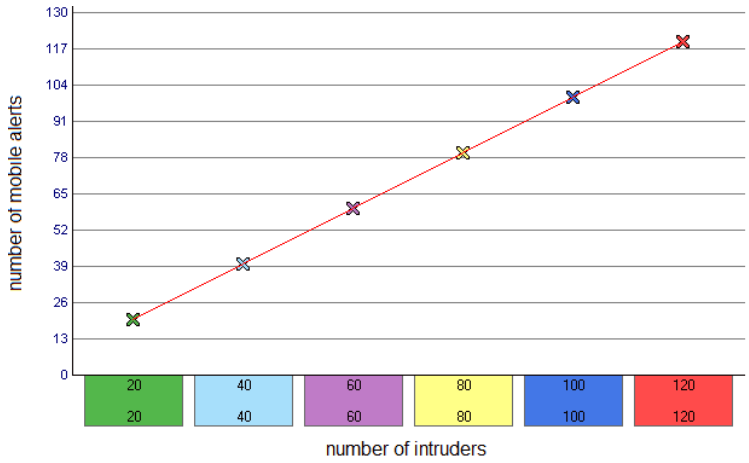

Fig 3: Security Analysis

The above graph depicts that the system efficiently provides the security and it can detect 'n' number of intrusions by alerting the user's and service providers immediately.

Performance analysis: In this section, we evaluate the performance of the proposed scheme under the security model defined earlier. We have tried accessing the cloud data from various devices simultaneously at the same time and got the same performance speed in accessing the data from the cloud even when there is an increase in number of accessing devices.

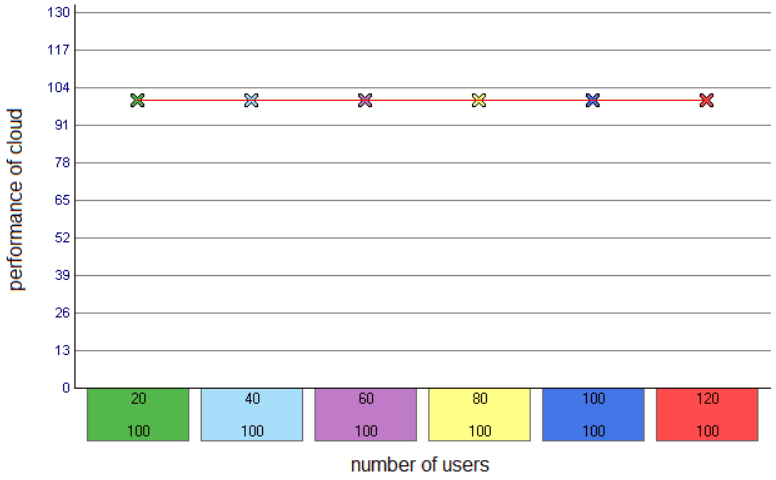

Fig 3: Performance Analysis

The above graph represents that this system efficiently provides security to 'n' number of users and its performance is constant even with the increase in number of users.

VI. CONCLUSION

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client.To ensure this, we proposed an effective and flexible distributed scheme that relies on the address authentication technique, and there by achieving the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). Also since we are not using the traditional key based algorithms, we have mitigated the risks of side- channel attacks. So use of "Address authentication" technique is highly essential in order to provide SECURED THIRD PARTY AUDITING in cloud computing.

REFERENCES

[1] IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No.5, May 2011-"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"

[2] IJCST Vol. 2, Issue 2, June 2011 –"Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud."

[3] IEEE INFOCOM 2010, San Diego, CA, March 2010 – "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing"

[4] IEEE July 2009 , Cong Wang, Qian Wang ,Kui Ren,Wenjing Lou – "Ensuring Data Storage Security in Cloud Computing"

[5] IEEE CCIS2011, Shuai Han, Jianchuan Xing "Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing"

[6] IJARST Vol. 4, Issue 2, August 2012, -" Third Party Auditing For Secure Data storage In Cloud Through Digital Signature Using RSA" (ISSN 2249-9954)

[7] IJARCSSE Vol. 3, Issue 3, March 2013 –" Using Third Party Auditor for Cloud Data Security: A Review" (ISSN 2277 128X)

[8] IJARCSSE Vol. 3, Issue 3, March 2013 –" Using Third Party Auditor for Cloud Data Security: A Review" (ISSN 2277 128X)

[9] Cross-VM Side Channels and Their Use to Extract Private Keys - CCS '12 Proceedings of the 2012 ACM conference on Computer and communications (Pages305-316) ISBN: 978-1-4503-1651-4

[10] Third Party Auditing in Cloud computing – NCPAM'14 Proceedings of 2014 National conference on Pure and Applied Mathematics, ISBN:978-93-83459-46-9

