Challenges and Mechanisms for Securing Data in Mobile Cloud Computing

Sharmila.R[1] Saravanan.P[2] Kokila.S[3]
[1,3]Research Scholar [2]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]D. B. Jain (Autonomous) Chennai-97, Tamil Nadu

Abstract— Cloud computing enables users to utilize the services of computing resources. Now days computing resources in mobile applications are being delivered with cloud computing. As there is a growing need for new mobile applications, usage of cloud computing cannot be overlooked. Cloud service providers offer the services for the data request in a remote server. Virtualization aspect of cloud computing in mobile applications felicitates better utilization of resources. The industry needs to address the foremost security risk in the underlying technology. The cloud computing environment in mobile applications aggravated with various security problems. This paper addresses challenges in securing data in cloud for mobile Cloud computing and few mechanisms to overcome.

Key words: Cloud Computing, Data Security, RSA, Cryptography, Email Security

I. INTRODUCTION

Cloud computing provides uncountable benefits to mobile applications of small size to larger size. In order to extend collaboration and innovation, business of all sizes deploys on mobile cloud computing. Use of cloud computing for mobile applications enables business volatility into single domain in addition to increasing technology effectiveness without increasing operational cost. With the support of cloud computing, mobile applications scale up on demand IT capacity and also have ability for managing large data sets. The use of cloud computing increasing day, the end users and the service providers are able to utilize the cloud resources with less cost and easily without owning all the resource needed. However, the services of cloud computing is having many problems associated with it. The most common is security. Since from last few years, the problems like security, authentication, privacy preservation, access control etc studied more by various researches [1]. CLOUD computing" implies access to isolated computing services suggested by third parties via a TCP/IP connection to the public internet. It is internet based development and use of computer technology. Public cloud, Private cloud and Hybrid cloud, which combine both public and private clouds are types of cloud computing [2].

A. Public Cloud

Public cloud provides scalable, dynamically provisioned, virtualized recourse available over the internet form an offsite third party provider. Think Grid is a company that provides multi-tenant architecture for supplying services such as Hosted Desktops. Other popular cloud vendors include Salesforce.com, Amazon EC2 and Flexi Scale.

B. Private Cloud

It is providing hosted services on the private networks. This type of cloud is used by large companies and allows their corporate network and data center administrators to effectively become in house service providers.

C. Hybrid Cloud

It combines resources from both internal external providers and so it becomes the most popular choice for enterprises. It is comprise of two or more than two clouds. There are three service models in cloud computing Software as-a-Service (SaaS), Platform as a-Service (PaaS) and Infrastructure as-a-service (IaaS).

II. LITERATURE SUPPORT

The key security issues concerned with cloud computing are being analyzed in the work of Eystein Mathisen[3]. Farzad Sabahi[4] discussed about the issues such as reliability and availability for cloud computing. The requirements and challenges that are faced by cloud service providers during cloud engineering are being the part of paper by Popovi and Hocenski[5]. Akhil Bhel [6] explores the applications to secure the cloud infrastructure and their drawbacks, Chang-lung Tsai et al.[7] proposed a mechanism that was not only focused on find out some solutions, but also focused on develop some feasible information security techniques or products for the application and service of cloud computing. Cloud service users need to be vigilant in understanding the risks of data breaches in the new environment. S. Subashini et al.[1] proposed a survey of the different security risks that pose a threat to the cloud.

A. Challenges behind Security Breach Cloud Based Mobile Computing Environment

1) Trust Related

As there is no means to access the mobile service provider's and cloud service provider's security level, users and stakeholders have no ability to measure the security level.

2) Loss of Data Related

The unaddressed issue to manage the loss of cryptographic management information can bring great damages to data leakage as well as data loss.

3) Data Integrity and Confidentiality Related

As the nature of cloud environment is based on virtualization feature, different mobile applications users share the same infrastructure which may lead to threat to data intergrity and confidentiality.

4) Data protection Inconsistency related

The decentralized nature of mobile cloud architecture may avenue threat to protection inconsistency in the manner in which access restricted by one module may be granted by smother.

5) CSA observations

"Cloud Security Alliance" (CSA)[9] discovered the top six security threats to cloud computing a

- Account, service and traffic hijacking

- Unidentified risk profile
- data leakage
- abuse use of cloud computing
- Malicious insiders
- API insecure

6) Networking Perspective threats

- XSS Attacks

There are two kinds of XSS attacks. There are Stored XSS and Reflected XSS. In Stored XSS, the noxious code is stored permanently in an asset handled by web application. On the other hand, in Reflected XSS, the noxious code is not stored permanently. Indeed it is instantly returned back to the client [10].

- Sniffer Attacks

These kinds of assaults are propelled by applications which can catch packets streaming in a network. If the information that is being exchanged through these packets are not encrypted, it can be perused. A sniffer program, through the network interface card (NIC) gat information or traffic attached to different frameworks on the network additionally gets recorded.

- SQL Injection Attacks:-

A harmful code is embedded into a standard SQL query. Therefore attacker gets an illicit access to a database. Attacker is capable to access or change some sensitive information of any cloud user or organization.

- Man-in-the-Middle Attacks:-

In such an assault, an intruder tries to meddle in a continuous discussion between sender and receiver to infuse false data and to have knowledge of the critical information exchange between them.

- Distributed Denial of Service (DDoS) Attacks:-

DDoS attack makes use of many machines and internet connections. Attacker uses a group of agents to send DDoS attack commands repeatedly to the target system. Sudden traffic can lead to load the website very slowly to their intended users. Sometimes this traffic is so high that it shuts down the site completely.

- Cookies poisoning

In order to access of an intruder to a webpage, it involves changing or altering the contents of cookie. User identity related credentials like username and password etc., are unauthorized user.

7) Threats behind Cloud Virtualization

Numerous bugs have been discovered in all prominent VMMs that permit getting least as of g into the host OS. All virtualization software at least as of now can be abused b harmful clients to sidestep certain security confinements. Virtual machine instance isolation guarantees that diverse instances running on the same physical machines are isolated from one another. Nonetheless, offering perfect is not possible by current VMMs.

Every client utilizes his identity for accessing cloud services. A major issue is unauthorized access to cloud asses and applications. A virulent element can imitate a real client and make use of cloud services. Numerous such malevolent elements acquire the cloud assets prompting un-accessibility of a service for real clients. Likewise it may happen that the client crosses his limit at time of service utilization in the cloud environment. This cloud be regarding access to safe zone in memory.

B. Mechanisms to Handle Threats

- Best security practices need to be implemented for installation and configuration on mobile cloud environment. Unauthorized changes and action needs to be monitored periodically. Strong authentication and access control needs to be enforced. Clients can impose service level agreement (SLA) for patching, regular scan for vulnerability and perform consistent audits.
- In order to handle Invective and Wicked Use of mobile Cloud Computing the registration and validation process must be full proof. Thorough monitoring of network traffic and credit card transactions needs to be done. Users can also analyze public prohibition list for someone's network block.
- Monitor security model of interfaces provided by cloud supplier for better Defending Unprotected Application Programming Interfaces (APIs). Ensuring robust authentication and access control can be effective during encrypted transmission and understanding the dependence chain related to APIs.
- Users can make use of strong two factor authentication technique as per requirements, and utilize proactive checking to recognize unauthorized activities. An alternate helpful venture to take is to understand policies of cloud provider and SLAs.
- There is a need to defend information loss with the mechanism. Successful measures are to encrypt and ensures integrity of information in transmission, analyze protection strong key generation during design and run time. Other possible steps to take are to execute strong key generation, managements, storage, destruction practices, contractually request suppliers to clean persistent media before it will be discharged into the pool.
- A sniffing recognition platform in view of ARP (address resolution protocol) and RTT (round trip time) can be utilized to recognize a sniffing framework running on a network. Use encryption mechanism to protect critical information, add MAC address of the gateway permanently to the ARP instead of IPV6 cache, use IPV4 and make use of SSH instead of Telnet, Secure copy (SCP) instead of FTP.
- Separate IDS is used for every cloud. Information exchange id the mode of working for different IDS over network. In the event when a particular cloud is under assault, the supportive IDS alert the entire system.
- Domain Name System Security Extensions (DNSSEC) diminishes the impact of DNS intimidations. In the situation when these efforts to establish safety turn out to be deficient when there is some malicious connection in between sender and receiver.
- Different techniques such: actualizing letter cover, variable textual styles of the letters used to plain a CAPTCHA, expanding the string length and utilizing a perturbative foundation can be keep intruder away from CAPTCHA breaking. CAPTCHA outline standards have been proposed, which will be capable to oppose any assault technique of static optical character recognition (OCR).

- Trust between the Service provider and the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk o insider attacks. This is a major issue and has received strong attention by companies [12].
- The service providers like Gmail, Yahoo Mail etc., require the username and password to use their services, but they are vulnerable to phishing attacks. IAM can be used to deal with this problem. It is a framework for business process for managing electronic identities. It supports management of multiple digital identities with their roles, authentication, authorization and privileges. Identity management system has different components like Identity authentication, Directory service, Password administration, Access management, User provisioning, Federated identities and Roles managements [13].

III. CONCLUSION

The potential value of mobile based cloud applications has opened the door for different security issues. The greater the bond between the user and the service provider is one of the approaches to reduce security breach. This paper made a study towards challenges towards mobile cloud computing and mechanisms to handle that. IT Security specialists must work towards to identify practical ways to protect security and privacy of mobile users.

REFERENCE

[1] Grobaur, B., Walloschek T., Stoker E.,(2011). Understanding Cloud Computing Inerabilities. Security and Privacy. IEEE, Vol.9,pp 50.
[2] Das Gupta et.al. Cloud computing based projects using distributed architecture, 201,PHI
[3] Eystein Mathisen. Securit Challenges and Solutions in Cloud Computing, in:
[4] International Conference on Digital Ecosystems and Technologies, IEEE DEST 2001, 2011.p.208-212.
[5] Farzad Sabahi. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks(ICCSN), May 2011.p.245-249.
[6] Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 proceedings of the 33rd International Convention, 2010.p.344-39.
[7] Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, 2011.p.217-222.
[8] Chang-Lung Tsai and Uei-Chin Li, Information Security of Cloud Computing for Enterprises, Advances on Information Service Sciences. Vol. 3, No.1, pp. 132-12, Feb 2011.
[9] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing., Journal of Network and computer Applications, Vol. 3, No .1. Jul, 2010.
[10] "Security Guidance for Critical Areas of Focus in Cloud Computing", April 2009, presented by Cloud Security Alliance (CSA).
[11] P.Vogt, F. Nentwich, N. jovanovic, E. Kirda, C.Kruegel, and G. Vigna.,(2014), cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In proceedings of the Network and Distributed System.
[12] Heiser, Jay and Mark Nicolett: Assessing the security risks of cloud computing Technical Report G00157782, Gartner Research, June 2008.
[13] http:/www.cloudcompetence center.com/understanding/ taxonomy cloud computing Security
[14] Nida, Pinki, Harsh Dhiman, 2014. A survey on Identity and Access Management in Cloud Computing. In Proceeding of International Journal of Engineering & Technology (IJERT).

