IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. III (Mar - Apr 2019), PP 12-16
www.iosrjournals.org

Mobile Cloud Computing Security Challenges and Method: A Review

Vipin Kumar
LPU Punjab India
Corresponding Author: Vipin Kumar

Abstract: *From the last few years mobile devices and mobile applications have grown exponentially. Also emerging of cloud computing opens the new way to building applications on on-demand infrastructures instead of building applications on fixed and rigid infrastructures. Cloud computing is very popular among companies as it provide the flexibility for creating on-demand infrastructure for developing custom applications. Accessing the company resources on mobile devices is also essential for growth of a business and makes quick decision.*
Cloud computing technology considered as very important for mobile services.MCC combine the cloud computing into the mobile environment and provide the benefits in terms of flexibility efficiency and strategic value. It also remove the limitations of mobile devices e.g., battery life, storage, and bandwidth from mobile environment. The security of the data and resources is also very necessary. This paper identify the challenges and review the method to make the uploading and downloading data between mobile device and network more secure, efficient and less power consumption.

Keywords: *Mobile cloud computing, Security, Cryptography, Encryption, Authentication*

Date of Submission: 27-03-2019 Date of acceptance: 12-04-2019

I. Introduction

Cloud computing is to use the remote machine services as per user requirements. The data store in cloud in encrypting form and if any company want to use this data for commercial product it first has to decrypt it.

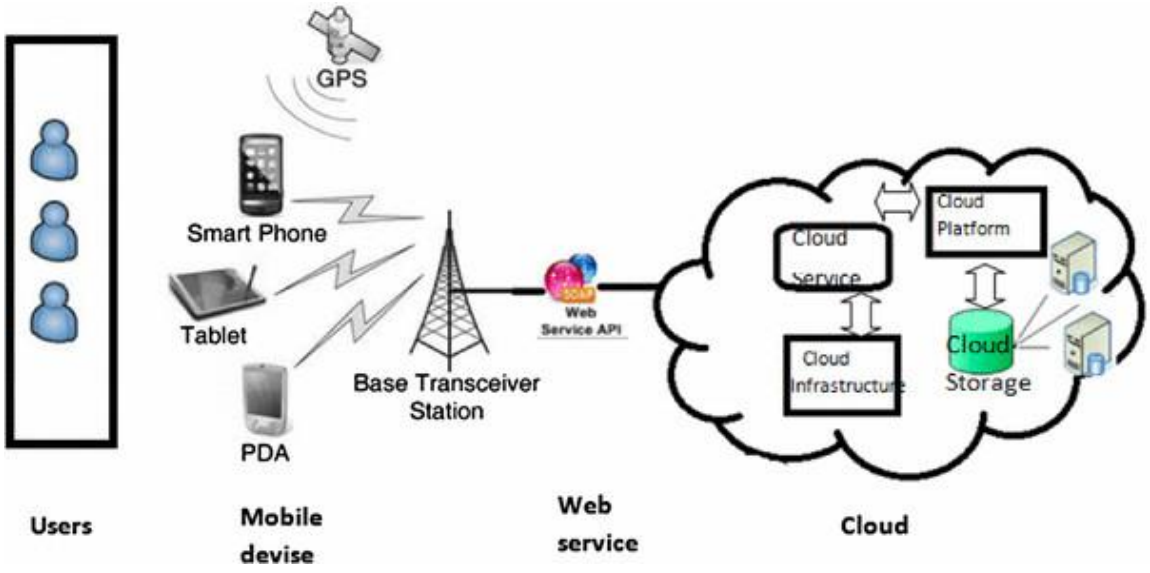
Security for any system is very important requirement, the fact is also true for cloud computing. Mobile cloud computing security is an emerging area and may be considered as sub domain information security. It has the same importance as computer security or network security. Cloud computing security consider as set of rules, policies, protocols and technologies that are used to secure applications, data, and associated infrastructure deploy on cloud platform.

Cloud service model can be divided into these three types

- Software as a Service also known as SaaS
- Platform as a Service also known as PaaS
- Infrastructure as a Service also known as IaaS

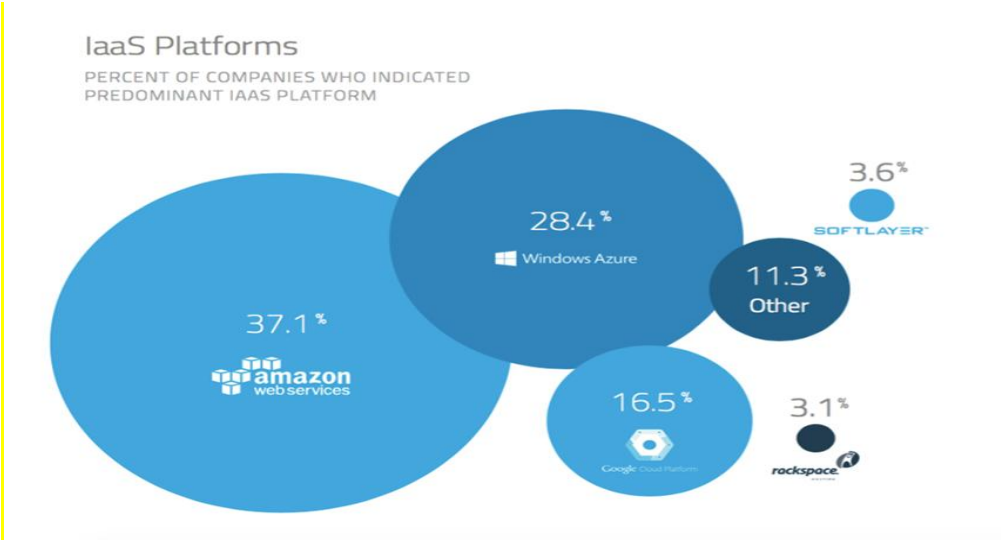
In the market there are also different types of cloud services provided as per user requirements like Private, Public, Hybrid and community. Private cloud can be used by individual person; whereas public cloud is open to all and any user who wants to use the resources can use that. There is a third type computing is hybrid cloud computing for a group of people [1].

Three entities involved in cloud computing: User to use data, company who provide data and cloud provider



In order to use fewer resources, cut costs, and maintain efficiency, Cloud Service Providers often store many customers' data on a single server. As a result, there is a chance that one user's private data can be seen by other users' possibly even competitors. In this situation data isolation and logical storage separation should be provided to handle such sensitive situations [2].

To store the data on public cloud by a company put the data on risk by outsider or insider attack. Or if an application host on public cloud it also have the possibility of insider attack. As per a recent report by a recent Cloud Security Alliance, insider attacks are the biggest threat in cloud computing.[3] Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data centre. Additionally some intruder detection system must be used and data centres must be frequently monitored for suspicious activity [4].



The full use of virtualization in implementing cloud infrastructure brings some security concerns for customers or tenants of a public cloud service [5]. Virtualization is implemented he relationship between the OS and underlying hardware - be it storage, computing or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured[6]. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist[7]. As an example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole data enter to go down or be reconfigured to an attacker's liking.

The responsibility of security is shared, however, the service provider must ensure that their infrastructure of cloud is secure and that their client's data and applications data are secured, while the user

must take measures to fortify their application and must not use weak passwords and authentication measures Endpoint security includes frequent patches for security vulnerabilities and endpoint-based security such as anti-virus, anti-spyware, host intrusion prevention, and host based firewall.

II. Security Challenges for cloud computing:

Security is essential part of any system and it is more important in system like cloud computing where data is stored at remote locations and freely available to use. These are the basic security challenges for MCC

1. Confidentiality and security of data at storage and in transit

Confidentiality ensures that certain information is only readable or accessible by the authorized party. Basically, it protects data from passive attacks. Transmission of sensitive information such as military information requires Confidentiality. Release of such information to advisory could have devastating consequences e.g. company information must also remain confidential so that rivalry could never take the advantages of identifying business strategy. With respect to the release of message contents, several levels of protection can be identified.

2 Authentication and identity

In any communication authentication is very important as every user must ensure that he is communication with correct user and information is not going to wrong hands. Generally password or PIN are used for user authentication but a well secure system must used some other method to authenticate the user .If authentication of user has not been done properly an attacker could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other user data on cloud [5].

3 Availability and fast speed

In cloud computing data stores at remote location and can be accessed only through network connections. If there is no reliable connections or user not able to reach his data there is the problem and the accessibility of data must be fast and delivery within time.

4 Integrity

Integrity of data defines as date must not modify in transition and guarantees that the authorized parties are only allowed to modify the messages or information. Some time message may be corrupted due to noise in the channel and data not remain as it is. Integrity also ensure correct data transmission between parties. Integrity can apply to a stream of messages, a single message or selected fields within a message. But, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under integrity service. Thus it addresses both message stream modification and denial of service [7].

5 Scaling

Most of the time it is not known in the starting about target audience and first things are started at lower level and later go on large scale. Scalability is related to security as the number of user increases, resources may become inefficient to handle these users. A mobile cloud network may consist of hundreds or even thousands of user data. Security techniques must be scalable for this type of networks. Otherwise, the newly added data in the network may be compromised by the attacker and used for gaining unauthorized access of the complete system.

6 limited computation capacity of mobile device

It is well known that the battery life and storage capacity of mobile devices is not adequate for processing of large business applications and also computation needed for these applications is out of reach for mobile devices. When a user wants to access the data from cloud to his mobile devices that may have limited battery file and processing power, it may be not work properly. So the algorithm and method for cloud computing should be such that they may take consideration of these situation and should be properly handled [12].

5. Method and new Technology for security in MCC

Some of the recent method reviews in this paper that is used for security in MCC. These method encrypt the data using any cryptography technique and use authentication code for user authentication and other credentials used to enhance security

1. Incremental cryptography

Incremental cryptography is the process to generate the hash code or MAC code for a message from the previously generated code. This scheme is very helpful in situation where there is very much limitations of computation speed and battery power like in mobile device. The idea was introduced by Bellare, Goldreich and Goldwasser in the papers [9]. The idea was further improved in [2] by dividing the file in different parts and compute the code for different prts.

F=f1 || f2 || f3 || f4 || f5 || f6...|| fn

Fj=DecryptEK(fi)(i<=j<=n)

2. Adaptive Authentication

According to author in [3] Risk-based authentication, sometimes called adaptive authentication, can most easily be described like a 2D matrix, whose elements represent the risk profile in combination. Based on these results additional security requirements finds and added to the previous result before implementation.

These functions, will typically find the unknown risks and and present as the matrix result. An example of these types of risk is in a login requests sensitive data capture or modification of security information. Both for internal network or systems access, as well as Web application scenarios.

3. Incremental password generator

Incremental password generator is a technique that supports the incremental update property. In case of insert a record into the file or delete a record from the file update the MAC value without generate the new Hash value. In [5] author present a incremental cryptography version of existing security scheme as coding based, sharing based and encryption based for improving block modification operations in terms of resource constrains.

4 Zero-day vulnerabilities

A zero-day exploit is an attack that exploits previously unknown security vulnerability. It takes advantage of early attack and attack on the same day , the day vulnerability is known. In [6] authors show the function and implementation and installation of zero-day vulnerabilities and use UNSW-NB15 dataset to shows the performance evaluation and checking the credibility in cloud environment.

5 Samsung weblet applications

Samsung provide a way to secure the mobile cloud applications by creating a separate module known as weblets. Weblet are software modules that are independent to each other and has a interface for communication and that can run on a device or cloud and interact user through user interface In [7] Zhang present a solution to secure an elastic mobile application [8] in cloud environment.

6 Identity based authentication:

Identity based authentication is based on behaviour of user and working pattern of user. It will be added as extra layer in existing security system. When a person comes to work and logging to system, he has some routine task and Identity based authentication take care of threads like address spoofing attack encryption, authentication and access control. In [10] author present a new protocol RDIC that is construction of identity-based (ID-based) that reduce the complexity of the system up to large extent. It uses the key-homomorphism cryptographic primitive and the cost for establishing and managing the public key authentication framework in the RDIC schemes based on PKI.

7. Proposed hypothetical technique:

Although many technique already exist but no one is full proof for all type of system. Available solutions customized and used as per requirements. A new type of security may be provided using the latest authentication technique using black of block chain in subsequent access of data [11].

8. Conclusion and Feature work:

Security of any system is very important and should be implemented carefully. Security in cloud computing is also very important because of data is uploaded on cloud and freely available. So the access control and authentication is very important in these types of mobile cloud computation system. There are many techniques to implement security in this type of system. Incremental password generator and incremented cryptography has the power to secure the any existing technique. Some applications have special techniques like Samsung weblet and Amazon hypervisors at the hardware level[13-15]. Providers must account for issues such as access policies, application deployment, and data access and protection to provide a secure, multi-tenant environment, technique to have limited access and full access only legitimate user. Now a day if company wants

to migrate to cloud they have only one fear of security of their data. A new research in the field of cloud security will increase the faith of stockholders.

Reference

[1]. Niroshinie Fernando , Seng W. Loke , Wenny Rahayu, "Mobile cloud computing: A survey ", June 20 12 Future Generation Computer Systems ,.

[2]. Abdul Nasir khan, M L mat khan "A study of incremental cryptography for security schemes in mobile cloude computing environment", IEEE 2013

[3]. Energy-Efficient Incremental Integrity for Securing Storage in Mobile Cloud Computing Wassim Itani Ayman Kayssi Ali Chehab

[4]. http://searchsecurity.techtarget.com/tip/Adaptive-authentication-An-introduction-to-risk-based-authentication

[5]. Abdul Nasir Khan, M L Kiah Samee U Khan "A Study of incremental cryptography for security scheme in mobile cloud computing environment" IEEE 2013 Symposium on Wireless technology and applicatin

[6]. Nour Moustafa, Gideon Creech, Elena Sitnikova, Marwa Keshk " Collaborative Anomaly Detection Framework for handling Big Data of Cloud Computing",

[7]. Securing elastic applications on mobile device for cloud computing", X. Zang, J Schiffman Proc. workshop on cloud computing security CCSW 09 Chicago IL USA Nov. 2009

[8]. R. K. Balan, M. Satyanarayanan, S. Park, and T. Okoshi, "Tactics-based remote execution for mobile computing". In Proc. of MobiSys, 2003.

[9]. Incremental cryptography: the case of hashing and signing M. Bellare, O. Goldreich and S. Goldwasser Extended abstract in Advances in Cryptology - Crypto 94 Proceedings, Lecture Notes in Computer Science Vol. 839, Y. Desmedt ed, Springer-Verlag, 1994

[10]. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage Y Yu, MH Au, G Ateniese, X Huang… - IEEE Transactions …, 2017

[11]. A First Look at Identity Management Schemes on the Blockchain P Dunphy, FAP Petitcolas - arXiv preprint arXiv:1801.03294, 2018

[12]. KhadijaAkherfia, MichealGerndta, HamidHarroudb "Mobile cloud computing for computation offloading: Issues and challenges " Applied Computing and Informatics Volume 14, Issue 1, January 2018, Pages 1-16

[13]. https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

[14]. WoonkiNaa, SeshaKovvuria, JonghoonKimb "Multi-Variate Discrete Wavelet Technique for Advanced State-of-Charge Estimation of a Lithium-Ion Cell " Energy Procedia Volume 105, May 2017, Pages 4525-4530

[15]. Zhang, Xinwen & Schiffman, Joshua & Gibbs, Simon & Kunjithapatham, Anugeetha & Jeong, Sangoh. (2009). Securing elastic applications on mobile devices for cloud computing. Proceedings of the ACM Conference on Computer and Communications Security. 127-134. 10.1145/1655008.1655026.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Vipin Kumar. " Mobile Cloud Computing Security Challenges and Method: A Review" IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 12-16.