Authentication Techniques for Mobile Cloud Computing and validates its Effectiveness

Rupali Tekade*, Prof. Kiran Agrawal** and Dr. Shishir K. Shandilya***
*-***Computer Science Department (Bansal Institute of Science and Technology, Bhopal)

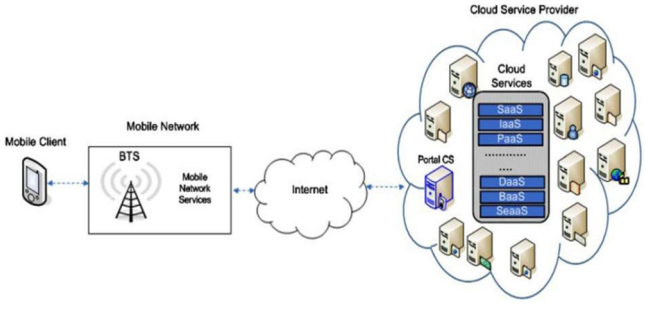
Abstract: Mobile Cloud Computing (MCC) consists wireless network, mobile device and cloud computing. In MCC the computation /storage resources of mobile device could capitalize using cloud server from different location via communication network. This untrusted communication network causes security and Authentication risk. Which needed a effective and powerful technique to overcome security breach problem. The objective of this paper is to study existing authentication techniques for establish the secure communication session between mobile devices and cloud server. And study of a security protocol analyzer called scyther which validates the effectiveness of the authentication scheme. Scyther analyzes a set of patterns and multi- protocol; it indicates the capability to protect from different security attacks such as man-in-the-middle, replay attacks, etc.

Keywords: Mobile Cloud computing, Mobile devices, Authentication, wireless network, Validation.

Introduction

The composition of cloud computing, mobile device wireless network and location-based services delivered are called Mobile Cloud Computing (MCC). Mobile devices access applications which executes partly in the mobile device and partly in the cloud server. It makes mobile device's computational ability more powerful. In MCC Applications run on the service provider's cloud server then sent to the user via the mobile browser. The development of multiple platform support mobile browser App on any mobile phone increases the number of users and App developers. Users hold multiple accounts with service providers such as Amazon, Google, e-Bay etc.

In spite of the success and popularity of MCC; mobility, authentication and security are the major issues, it requires strong and lightweight security and authentication process. This is a complex task across organizations where different Delivery platform and service model requires different measure.



Mobile cloud Computing allows user to store their enormous amount of data to the cloud server with low cost, good reliability, availability and without doing complex management of storage hardware. Mobile device have become an essential part of human life. Demands of dense and complex activities require a reliable and practical computing device, Mobile device provide best solution using mobile cloud computing to solve large complex problems. Beside the growth of mobile cloud computing it is not increase the trust of user in the cloud-based data management, especially among businesses because of the risk of security and privacy. The threat becomes an obstacle to adapting mobile cloud computing paradigm. Therefore, it is necessary to build strong security system that can reduce the risks of security and privacy in MCC.

There are three types of service model provided by mobile cloud computing to mobile device user. It has increased the productivity of a variety of different fields.

• *Software as a Service (SaaS)* - It included cloud based software and application such as cloud based antivirus and word processing software. The applications are accessible from various client devices through a web browser. The user does not manage or control cloud infrastructure including network, servers, storage. eg, Yahoomail, Dropbox, Google Docs.

• *Platform as a Service (PaaS)* - Platform as a service allows product deployment on the cloud created by consumers using programming techniques and tools. The consumer has control over the deployed applications.eg: Google App Engine, Microsoft Azure, Android (Google PlayStore), Facebook.com (application services and online gaming)
• *Infrastructure as a Service (IaaS)* -This service provided to consumer to process, store, and perform important basic computing, where client can deploy and run the software freely include operating systems and App. eg. Host firewalls , EC2, S3.

Related Work

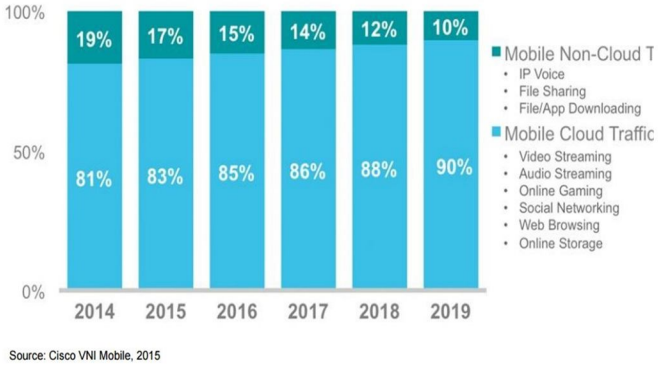
Zhang et at. Propose a new type based proxy re- encryption security scheme to enhance security feature of mobile cloud computing. In mobile cloud computing the data distribution system has lightweight and easily deployable solution for mobile users since does not involve any trusted third party. Each mobile user only has to keep a short secret key. Thus, it provides properties include data privacy, data integrity, data authentication , dynamic data modification as well as the access control. Type-based proxy re-encryption scheme is based on Merkle hash tree, as well as BLS signature to ensure the security. Performance and proof-of-concept implementation of this scheme makes data distribution practical. [3]
M. Arfan et al. describe the secure data trans- mission scheme based on cryptographic hash function. The data distribution goes through hash encryption Mechanism, Every line of plaintext will be transmitted in encrypted complex form that can't be readable directly. In MCC the hash algorithm based encryption process make it difficult for hackers to retrieve the information. And also the use of Virtual machine can improves the data security of mobile cloud application and act as the security engine to sent bits of data. With this system, the corporate and individual user can manage business resources online quickly and safely from the risks of data leakage. [2] Shaikha et al. describe the data classification technique to deal with the data security and privacy issues of data storage in cloud. A set of parameters are needed for data classification in cloud which provides security levels based on type of content and accessibility .Parameters are defined is based on dimensions. The level of security in cloud storage is given as per the confidentiality and access restriction required for the specified data. Based on the data classification on proposed parameter for storage and communication encryption, integrity and access control mechanism are performed. A regularized backup plan can be decided for disaster and recovery. Data security and quality standard improves the strength substantially. The efficiency of the data classification scheme is analyzed with the collected sample dataset. [5]
Han et al. proposed the model of effectively enhancing user's data and privacy, security in mobile cloud computing environment through quantum cryptography technology. Existing classical optical fiber network can be conveniently upgraded to quantum key distribution network. After quantum keys distributed it will forward to the mobile users by NFC technology. Mobile users can use the quantum cryptography technology to communicate with applications on the cloud after authentication process.[10]
IehabALRassan et al. MCC introduced some security threats such as unauthorized user access beside its popularity. The focus of the research is to protect from illegitimate access of mobile cloud and its resources using fingerprints to prove the users identity. combine each fingerprint with a password to form a multiple passwords scheme . The password consists from the finger sequence in the hand (left or right) plus a fixed password; this will make the passwords to be easy to remember. The results showed that this scheme is very strong and difficult to break it. The solution for authenticating mobile cloud users using the existing mobile device camera as a fingerprint sensor to obtain a fingerprint image, then process it and recognize it.[13] [21]
Babaeizadeh et al. This paper present keystroke dynamic authentication(KDA) in mobile communication. It has described a new biometric method based on measuring keystrokes duration. It helps to identify users based on their unique behavioral biometric along with passwo- rd. Keystroke analysis does not require the aid of extra special tools, therefore it is cheaper than other biometric methods. It is explained that performance metric can use for measuring keystrokes, this naturally bring the idea of improving KDA by measuring False Rejection Rate (FRR). It is percentage of attempts of wrongly recognize- ing a legitimate user as an imposter. if unauthorized person knows the username and password of legal user, can not gain access rights because of difference between their keystroke duration. Therefore, it is hard for an attacker to pretend as an owner.[19]
Audithan et al. This scheme enables the users to access multiple service providers with a single private key. Instead of opting traditional public key cryptosystem like RSA, it uses bilinear pairing technique for effective anonymous authentication. This scheme supports mutual authentication, mobile cloud users and service providers are only allowed to communicate during the authentication process. The third party is considered to be trusted and it participates in the registration, it prevents the malicious mobile users and service providers.[20]

Theory

Validation of Effectiveness of Authentication technique: The prerequisite process of mobile cloud computing is mobile device has to be register with cloud server before accessing cloud services. The data trans- mission between mobile device and cloud server has taken once they authenticate each other, this will ensure secure communication between two legitimate parties. It is not suitable for mobile device to perform authenticati- on process like complex operation because of lack of

computational capability. Thus it require a single step authentication scheme. The effectiveness of the authentication scheme is validated by security protocol analyzer called scyther. also calculated the vulnerability score to determine the vulnerability of the system. The value of score lies between 0.0 and 1.0.The lower the value indicates higher the security. Figure 14 indicates the increasing mobile data traffic and popularity of using mobile cloud computing paradigm, Thus it is very necessary to validates the authentication scheme to ensure the data protection from illegitimate user.

Figure 14. Cloud Applications Will Account for 90 Percent of Mobile Data Traffic by 2019



Source: Cisco VNI Mobile, 2015

A research can be performed by performing surveys, field study, experiments, computer simulation etc. Considered computer simulation to validate authen- tication scheme using *Scyther* as a part of the security analysis to launch attacks on the authentication scheme. *Scyther* analyzes a protocol once it is written in *Scyther* coding format. It accepts a minimum of two roles, where one role represents an initiator or sender and the other role represents a receiver. It allows us to define what type of key is used in the protocol, such as symmetric key, or asymmetric key, in addition it allows us to define whether a parameter is constant or variable. Once the protocol is defined, configure the attack scenarios. It has many predefined attack scenarios, which are used to test whether a protocol lacks confidentiality and integrity.

Compute a vulnerability score and perform a security analysis of the scheme to describe how secure it is. Let Nt is the number of attacks that are launched on the proposed scheme and *Ns* is the number of successful attacks that are recorded. Then, the likelihood of successful attacks on the scheme defines its vulnerability score = Ns / Nt .

Scyther is configured from the setting option to launch all types of attacks. In order to compromise the system, during the execution of each run, *Scyther* tried to launch different types of attacks considering hackers have initial knowledge of the system. We made various security claims, which are validated by running our proposed scheme using *Scyther*.

Conclusion

Mobile Cloud Computing is a combination of wireless network, mobile device and cloud computing. In the field of Information technology, ecommerce, healthcare and transportation etc. have significant benefits of mobile cloud computing. Because of popularity of Mobile devices and its low computing ability MCC have emerge area in the field of technology. The large amount of data storing and data computation occur outside the mobile device. Despite the advantages of this innovative compu- ting model, MCC could suffer security problem because mobile devices access services from different geographical location ,from untrusted network. To Get the best authentication scheme it is necessary to calculate the vulnerability score to check the effectiveness of the scheme. A security protocol analyzer scyther tool is used to getting the result of effectiveness.

Future Work

The computation overhead of mobile device would be reduced if single authentication scheme is used for secure communication. It is not suitable for mobile device to perform complex operation of authentication process because of lack of computational capability.

Reference

[1] Nitin Naik and Paul Jenkins(2016), A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards,2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.

[2] M. Arfan, Mobile Cloud Computing Security Using Cryptographic Hash Function Algorithm.

[3] Jiang Zhang,Zhenfeng Zhang and Hui Guo(2017), Towards Secure Data Distribution Systems in Mobile Cloud Computing, DOI 10.1109/ TMC.2017 .2687931, IEEE Transactions on Mobile Computing.

[4] Saurabh Dey,Srinivas Sampalli and Qiang Ye (2016), MDA: message digest-based authentication for mobile cloud computing, Dey et al. Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:18 DOI 10.1186/s13677-016-0068-6.

[5] Rizwana Shaikha, Dr. M. Sasikumarb(2015),Data Classification for achieving Security in cloud computing, Procedia Computer Science 45 (2015) 493 – 498.
[6] Nabeel Khana, Adil Al-Yasirib(2016),Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework, Procedia Computer Science 94 (2016) 485 – 490, The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies(IoTNAT' 2016).
[7] Khadija Akherfi, Micheal Gerndt , Hamid Harroud (2016), Mobile cloud computing for computation offloading: Issues and challenges.
[8] Patricia T. Endo, Moisés Rodrigues, Glauco E. Gonçalves, Judith Kelner, Djamel H. Sadok and Calin Curescu(2016), High availability in clouds: systematic review and research challenges, Endo et al. Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:16 DOI 10.1186/s13677-016-0066-8.
[9] Abdul Razaque and Syed S. Rizvi(2017),Privacy preserving model: a new scheme for auditing cloud stakeholders, Razaque and Rizvi Journal of Cloud Computing: Advances, Systems and Applications (2017) 6: DOI 10.1186/s13677-017-0076-1.
[10] jiawei Hanl ,Yanheng Liul ,Xin Sun, Lijun Song, Enhancing Data and Privacy Security in Mobile Cloud Computing through Quantum Cryptography.
[11] SUGANYA V SHANTHI A L(2015), Mobile Cloud Computing Perspectives and Challenges, International Journal of Innovative Research in Advanced Engineering (IJIRAE)ISSN: 2349-2163 Issue 7,Volume 2 (July2015).
[12] Nirbhay K. Chaubey, Darshan M. Tank(2016) Security, Privacy and Challenges in Mobile Cloud Computing (MCC):- A Critical Study and Comparison, Vol. 4, Issue 2, February 2016, ISSN(Online): 2320-9801,ISSN (Print): 2320-9798.
[13] IehabALRassan, HananAlShaher(2013), Securing Mobile Cloud Using Finger Print Authentication International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.6, November 2013 DOI: 10.5121/ijnsa.2013.5604 41.
[14] SIVARAMAN AUDITHAN,VIJAYAREGUNATHAN VIJAYASARO, PANDI VIJAYAKUMAR, VARADARAJAN VIJAYAKUMAR (2016),An Efficient Authentication Scheme for Mobile Cloud Computing Services, JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 32, XXXX-XXXX (2016).
[15] Mrs. S. M. Barhate, Dr. M. P. Dhore, User Authentication Issues In Cloud Computing, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 30-35
[16] Amazon S3, http://aws.amazon.com/s3/.
[17] Cisco visual networking index: Global mobile data traffic forecast update, 2013–2018, February 5, 2014.http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ visual-networking-index-vni/white paper c11-520862.html.
[18] MIRACL Crypto SDK, https://certivox.com/. Secure Hash Standard (SHS), National Institute of Standards and Technology (NIST), FIPS PUB 180-4, http://csrc.nist.gov/publications/PubsFIPS.html.
[19] Mahnoush Babaeizadeh, Majid Bakhtiari, Mohd Aizaini Maarof(2014), Keystroke Dynamic Authentication in Mobile Cloud Computing ,International Journal of Computer Applications (0975 – 8887) Volume 90 – No 1, March 2014 ,29
[20] Alaa Hussein Al-Hamami, Jalal Yousef AL- Juneidi,2015, Secure Mobile Cloud Computing Based- On Fingerprint,World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221- 0741 Vol. 5, No. 2, 23-27, 2015 .
[21] SUNEELA MADHAVI ATMAKURI (2015), CMI, A STUDY OF AUTHENTICATION TECHNIQUES FOR MOBILE CLOUD COMPUTING.
[22] Shakti Shivalingam, Ranjana Rai, MOBILE CLOUD COMPUTING: ARCHITECTURE AND SECURITY ISSUES International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 279-282 279 . [25] Mrs. Yogita D. Mane ,Prof. Kailas K. Devadkar,2015 , Protection concern in Mobile Cloud Computing- A Survey ,IOSR Journal of Computer Engineering (IOSR-JCE) ISSN : 2278-0661, ISBN : 2278-8727, PP : 39-44 (SICETE) 39
[23] E. Sasi1, R. Saranya priyadharshini ,SECURED BIOMETRIC AUTHENTICATION IN CLOUD SHARING SYSTEM ,International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March- 2015, pg. 572-577, ISSN 2320–088X.
[24] Adrian Covert. "Google Drive, iCloud, Dropbox and more compared: Whats the best cloud option?",2012. http://gizmodo.com/ 5904739.
[25] Secure Hash Standard (SHS), National Institute of Standards and Technology (NIST), FIPS PUB 180-4, http://csrc.nist.gov/publications/PubsFIPS.html.