Proceedings of the International Conference , Computational Systems for Health & Sustainability
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

A Review and Research towards Security in Mobile Cloud Computing

Chandan J
M.Tech , Software Engineering
RVCE, Bengaluru.

Asha B Patil
M.Tech , Software Engineering
RVCE, Bengaluru.

Dr Jitendranath Mungara
Professor & Dean PG studies,ISE
RVCE, Bengaluru.

Abstract: Mobile cloud computing is a combination of cloud computing and mobiles. Mobile cloud computing represents an infrastructure where data processing and storage of the data happens away from the mobile device because of the limited resources which is provided by the mobile infrastructure. Total of 42.8 million (1.1% of total mobile users) people are Mobile Cloud Computing users in 2008 which will be about 998 million (19% of total mobile users) by 2015. This is because of the reason of security and cost. Most of the IT Executives and CEOs are not willing to adopt the MCC infrastructure because of the security concern. Inspite of many efforts and research which has been made there are many loopholes and challenges which are still present. In this paper we present the security aspects and possible solutions for the same.

Keywords: Mobile Cloud Computing (MCC).

INTRODUCTION

There are few disadvantages with the mobile equipments, they are

- Limited storage capacity
- Limited Calculation ability
- Poor battery's sustainability
- Poor data sharing ability with PC[1]

To overcome all these problems we comeup with the MCC infrastructure which enables huge computing by data offloading to the server or to the cloud infrastructure.

In any MCC infrastructure we have Mobile Terminal, Mobile Network and cloud which provide services.There are series of services provided they are Infrastructure as a service(IaaS), Software as a service(SaaS), Platform as a Service(PaaS). The following figure represents the MCC Model.

In the recent era the research in mobile cloud computing in being widely done both in the academic field and industry. MCC is a service provided on demand on pay on use basis.MCC provides a facility of accessing the data from anywhere by the finger tips.

There are a several research which is done on the following area:

How to extend the battery life of mobile devices?

How to extend the limited resource of mobile devices?

How to solve the wireless bandwidth limited and delay?

How to ensure that security and privacy of MCC?[1]

Challenges	Solutions
Limitations of mobile devices	Improvement of processing capacity, storage, battery time of mobile devices
Quality of communication	Bandwidth upgrading, Data delivery time reducing
Division of applications services	Fast optimization algorithm techniques based on which tasks to be shifted onto the remote servers

Table1:Challenges and solutions for MCC

Figure 1: Overall view of MCC Challenges

SECURITY AND PRIVACY ISSUES IN MCC

We have three types of basic security concerns which are present in MCC infrastructure. They are

- MCC Technical challenges
- MCC security challenges
- MCC Micellaneous challenges[2]

Each one has several security issues which has to be dealt with.

A.MCC Technical challenges

- Data latency
- service availabilityHeterogeneity
- Adapting to networks shifts and platforms
- session management in cloud
- Compatibility of Cloud services model
- Computation offloading tradeoff
- compartmentalized data access
- Data caching
- Content delivery
- Maintaining confidentiality of data, access control and identity management

Security issues		Current approaches
Mobile terminal	Malware software	Detection and prevention CloudAV
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others(lack of security awareness, mis-operation)	Regulating the users' behavior
Mobile network	Information leakage or Malicious attack	Data encryption
		Security protocol
Mobile cloud	Platform reliability	Integrating the current security technologies;
	Data and privacy protection	Key management and data encryption; Authentication and access control Privacy and data protection

Table 2: Security Issues and corresponding currrent apporches.

B. MCC Security challenges

- Cloud Service Challenges
  - Malicious content injection
  - Attack on service availability
  - Integrity of data in cloud
  - Access to data on cloud storage
  - Takeover of Cloud management system
  - Risks of multi-tenancy
  - Insecure APIs by vendors
  - Design Flaw in service model
- Communication Channel Challenges
  - Data Leak
  - Data Tampering
  - Repudiation Issues
- Mobile Application challenges
  - Unauthorized cloud access
  - Access to Private data on mobile
  - Attack on Application availability
  - Introducing malicious content
  - Introducing malicious scripts
  - Risk of multi-tenency

C. MCC Miscellaneous Challenges

- Network Accessibility
- Compliance of the cloud[2]

SECURITY IN MCC USING BIOMETRIC AUTHENTICATION

There are ways of providing security in MCC using passwords[3] in a single stage or at multistage[5], by handwriting of the user, quick response codes, or combination of these[4].

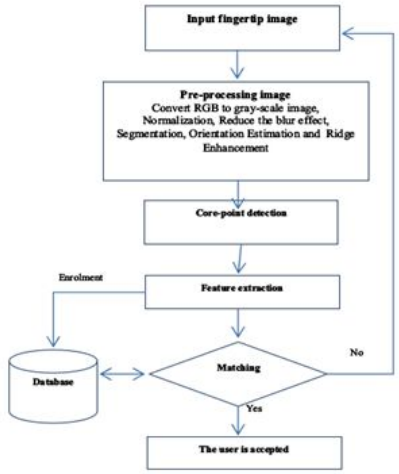

Figure 2: Biometric authentication process.

The use of biometric authentication can also be done using the camera of the smartphone. Then we convert the captured image and process the same in many stages to obtain ridge. The following flow chart will explain the process of biometric authentication.

Intially, in the enrollment phase the user presents the application with few of his fingerprint samples which is stored in the database for the comparision and identifying the user. The matching function extracts the features which are needed for matching. If matching is accepted then user is accepted else not. The Similarity score(S) is the outcome of comparision with the predefined threshold(T).

```
IF(S IS A LOW VALUE)
THEN
    LITTLE SIMILARITY
IF(S IS HIGH VALUE)
THEN
    HIGH SIMILARITY
IF(S>T)
THEN
    THE USER IS ACCEPTED
ELSE
        THE USER REJECTED
```

SECURE DATA STORAGE IN MCC USING RSA AND HASH FUNCTION

To ensure the correctness of users' data in the cloud, using an efficient mechanism of RSA and hash functions with features like data integrity and confidentiality which provide better security of the data stored by the user.

The participants in the above stated protocol are mentioned in the table below.

Participant	Role
Data Owner (DO)	Data owner is a person who utilizes the storage services provided by the cloud service provider.
Third Party Auditor (TPA)	TPA checks the integrity of the data stored on mobile cloud.
Cloud Service Provider (CSP)	CSP provides the storage services to the mobile users.

Table 3: Participants and there roles.

The protocal is similar to that of the RSA cryptographic algorithm using public and private keys. In cloud we store the encrypted file which is sent to the user and decrypted using his private key. Encrypted files are stored in the CSP.

The encryption and decryption of the data files are similar to that of the RSA mechanism.

PARTICIPANT	STORAGE REQUIREMENT
MOBILE DEVICE	Stores Public key of TPA and Public and Private key of owner
TPA	Stores Public key and private key of itself and Hash of the file received from mobile user
CSP	Stores encrypted file of mobile user

Table 4: Participants and there storage.

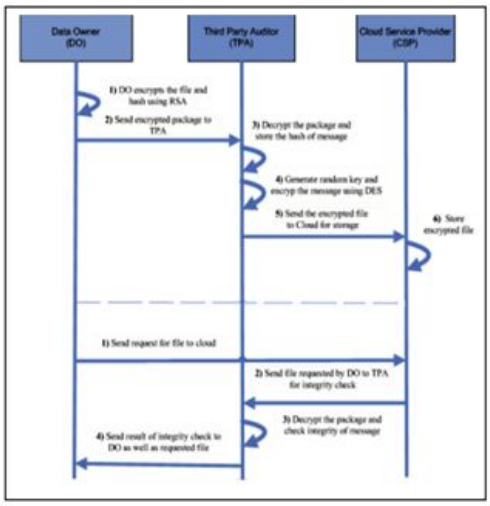

Figure 3: interaction among the participants.

ALGORITHM 1: Set Up

TPA: pk1, d1= GenKey()
Client: Pk2, d2= GenKey()
TPA → Client: d1
Client: F'= (E (F, d2)), H(F') = H(E (F, d2)) F"= E (F', d1),
H'(F')=E (H(F'), d1)
Client → TPA: F"| H'(F')
TPA: Store(H'(F')), k=Random(), F'= D(F",pk1),
F"=Encrypt(F',k)
TPA → CSP: F"
CSP: Store(F")

ALGORITHM 2: Verification

CSP → TPA: F"
TPA: F'= D (F", k), newH'(F')=H(F'), retrieve(H'(F')),
H(F')=D(H'(F'),pk1), Result= Compare (H(F'), newH'(F'))
TPA → Client: Send (Result)

ALGORITHM 3: Message Retrieval

Client → TPA: Request (F)
TPA → CSP: Request (F")
CSP → TPA: Send (F")
TPA: Verification (F"), F'=E (F, d2)
TPA → Client: Send (F')

The above procedures depict the process which is being implemented by the algorithm.The algorithm ensures correctness, authentication, privacy and confidentiality.

CONCLUSION

When we have limited resources we face many problems regarding the security. Implementation of any of the above stated apporches we can solve the problem wrt security and privacy. There will alwaya be scope for enhancements which will take place in further span of time.

ACKNOWLEDGEMENTS

The authors would like to thank every one whose support were of immense help during the development of this paper.Special thanks to the support and institutional facilities provided by R V college of Engineering and Department of Information Sciemce and Technology, RVCE.

REFERENCES

[1]. Hui Suo,Zhuohua Liu,Jiafu Wan,Keliang Zhou, "Security and Privacy in Mobile Cloud Computing."

[2]. PinkuHazarika,VinodBaliga, Seshubabu Tolety "The Mobile Cloud Computing Roadblocks"

[3]. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011, pp. 110-115.

[4]. D. S. Oh, B. H. Kim, and J. K. Lee, "A Study on Authentication System Using QR Code for Mobile Cloud Computing Environment," Future Information Technology, pp. 500-507, 2011.

[5]. H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," in Computing, Communication andApplications (ICCCA), 2012 International Conference on, 2012, pp. 1-4.

