International Research Journal in Advanced Engineering and Technology (IRJAET)

ISSN (Print) : 2454-4744 | ISSN (Online) : 2454-4752 (www.irjaet.com)

Vol. 1, Issue 1, pp.54-60, June, 2015

Security and Privacy issues in Mobile Cloud Computing and its Perspectives

M. Kumari Kala, AP/CSE, S. Aarthi, AP/CSE, S.Yuganya Devi, AP/CSE.
Department of Computer Science & Engineering
Sri Krishna College of Engineering, Arakkonam- 631003

ARTICLE INFO

Article History:

Received 2nd, Sep, 2015
Received in revised form 8th, Sep, 2015
Accepted 25th, Sep, 2015
Published online 26th, Sep, 2015

Keywords:

Mobile Phone, tablet, fablet, Cloud Computing, Security and Cryptography.

ABSTRACT

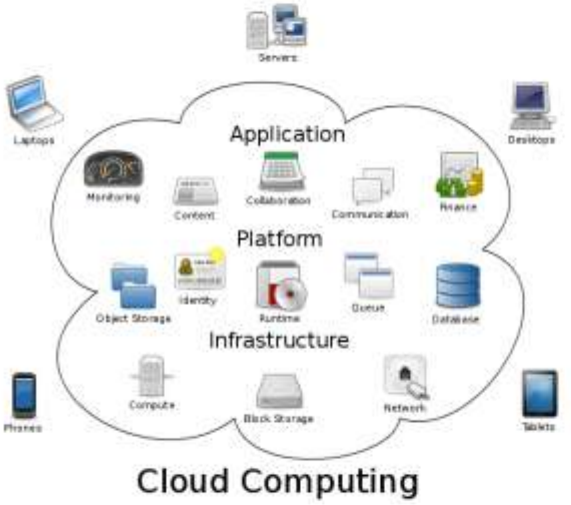
Abstract:-Now days the market of mobile phone is growing at a very high speed. Everyone has a mobile, tablet, fablet, (tablet with calling facility).Together explosive growth of the mobile applications and emerging of cloud computing concept, mobile cloud computing (Mean introduced to be a potential technology for services. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related computing. Security is another key issue that needs to be considered, which comes into picture once the communication channel is setup. Most of them are based on the public and private key cryptography. Specifically, we discuss the security problems in wireless systems and the proposed solutions and security measures implemented in several wireless systems. This paper gives a information about mobile cloud computing application, security, issues. The issues, existing solutions and approaches are presented.

I OVERVIEW OF MOBILE COMPUTING

The term of mobile computing is often used to describe this type of technology, combining wireless networking and computing. Various mobile computing paradigms are developed, and some of them are already in daily use for business work as well as for personal applications. Wireless personal area networks (WPANs), covering smaller areas (from a couple of centimeters to few meters) with low power transmission, can be used to exchange information between devices within the reach of a person. In ad-hoc (also known as peer-to-peer) mode (Figure 1.1), connections between two or more devices are established in an instantaneous manner without the support of a central controller. The client-server mode is chosen in architectures where individual network devices connect to the wired network via a dedicated infrastructure (known as access point), which serves as a bridge between the mobile devices and the wired network. This type of connection is comparable to a centralized LAN architecture with servers offering services and clients accessing them.

1.1 What is Mobile Cloud Computing?

Mobile Cloud Computing Forum defines MCC as Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing .



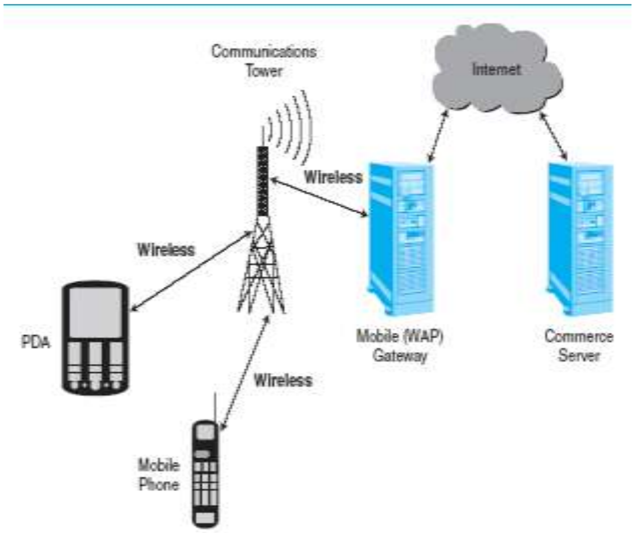


Figure 1.1 Mobile Computing infrastructure

Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services regularly available on the wide area network [2]. Due to its inherent infrastructure-less and self-organizing properties, an ad hoc network provides an communications in situations where geographical or terrestrial constraints demand totally distributed network system, such as military tracking, hazardous environment exploration, reconnaissance surveillance and instant conference. While we are enjoying the various services brought by mobile computing , we have to realize that it comes with a price: security vulnerabilities.

1.2 ADVANTAGES OF MOBILE CLOUD COMPUTING

Cloud computing is known to be a promising solution for Mobile computing due to many reasons (e.g., mobility, communication, and portability .In the following, we describe how the cloud can be used to overcome obstacles in mobil computing, thereby pointing out advantages of MCC.

CLOUD COMPUTING BENEFITS
High level computing
Secure storage & management
Low Total cost Ownership
Location independent
Utility - based Time-sharing models
Scalability & Sustainability
Pay-as- you- use
24/7 Support
Virtualized & Dynamic
Agile Deployment

II SECURITY MEASUREMENT IN MOBILE COMPUTING AREA

Secure mobile computing is critical in the development of any application of wireless networks.

Requirement of Security

Similar to traditional networks, the goals of securing mobile computing can be defined by the following

Attributes: availability, confidentiality, integrity, authenticity and non-repudiation.

Availability ensures that the intended network services are available to the intended parties when needed.

Confidentiality ensures that the transmitted information can only be accessed by the intended receivers and is never disclosed to unauthorized entities.

Authenticity allows a user to ensure the identity of the entity it is communicating with. Without authentication, an adversary can masquerade a legitimate user, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of users.

Integrity guarantees that information is never corrupted during transmission. Only the authorized parties are able to modify it.

III ISSUES IN MOBILE CLOUD COMPUTING

Cloud is extremely powerful to perform computations while computing ability of mobile devices has a limit so many issues occur to show how to balance the differences between these two. So there are some issues in implementing cloud computing for mobile. These issues can be related to limited resources, related to network, related to security of mobile users and clouds [4]. Some issues are explained as follows: 3.1 Limited Resources Having limited resources in mobile device make use of cloud computing in mobile devices difficult. Basic limitations related to limited resources are limited computing power, limited battery and low quality display. 3.2 Network related issues All processing in MCC is performed on the network. So there are some issues related to the network like Bandwidth, latency, availability and heterogeneity 3.3 Security Most of mobile devices have almost same functionalities like a desktop computer. So mobile devices also have to face a number of problems related to security and privacy. To overcome this problem threat detection services are now performed at clouds but this also has to face a lot of challenges. Some security issues are like device security, privacy of mobile user and securing data on cloud etc.There are so many security threats like viruses, hacking, Trojan horses in mobile devices also. The use of global positioning system (GPS) in mobile devices gives birth to the privacy issues.

IV MOBILE HOST PROTOCOLS

In order to deal explicitly with the concept of computers that move, new communications protocols are needed. The current assumptions made in protocols for the fixed network may no longer be valid due to the effects of mobility. The developments of protocols for locating a mobile host are currently under way. [3] These protocols attempt to make the operation and performance of a mobile host indistinguishable from that of a fixed host. This goal translates into two essential requirements: operational transparency and performance transparency above IP.

V NECESSITY OF CYBER SECURITY INFORMATION

Information is the most valuable asset with respect to an individual, cooperate sector, state and country. With respect to an individual the concerned areas are: 1) Protecting unauthorized access, disclosure, modification of the resources of the system. 2) Security during on-line transactions regarding shopping, banking, railway reservations and share markets. 3) Security of accounts while using social-networking sites against hijacking. 4) One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses [5]. 6) Need of separate unit handling security of the organization. 7) Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness [14]. 8) In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered [15]. 1) Securing the information containing various essential surveys and their reports. 2) Securing the data basis maintaining the details of all the rights of the organizations at state level. Development of operating systems, software layers, and downloadable apps.

VI SECURITY IN MOBILE CLOUD COMPUTING

Security framework in Mobile Cloud Computing cloud computing is growing day by day due to the popularity of cloud computing and increasing uses of mobile devices. Many researchers are showing their interest towards this technology. There are many issues in mobile computing due to many limitations of mobile devices due to low battery power, limited storage spaces, bandwidth etc.Security is the main concern in mobile cloud computing.

Security in mobile cloud computing can be

Security of data/files

The main issue in using mobile cloud computing is Securing the data of mobile user stored on mobile cloud.

Why data storage security is needed ?

The data of owner is stored on the cloud server; once the data is stored the owner does not have that data on his own device. Thus, there is risk related to data security and confidentiality of the data.

VII SYMMETRIC-KEY AND ASYMMETRIC CRYPTOSYSTEMS

In a symmetric-key cryptosystem, the encryption and decryption keys are the same. Since the encryption and decryption transformations are easily derivable from each other, a common secret key is shared between the communicating entities in advance via a secure 3 channel. Therefore, the security of symmetric-key cryptosystems depends on keeping the key secret. Some of the most important symmetric-key cryptosystems that are used presently are the American Data Encryption Standard (DES) and the Japanese Fast Data Enciphering Algorithm (FEAL). In an asymmetric-key (public-key) cryptosystems, the encryption and decryption keys differ. Each user has a private key and a public key.

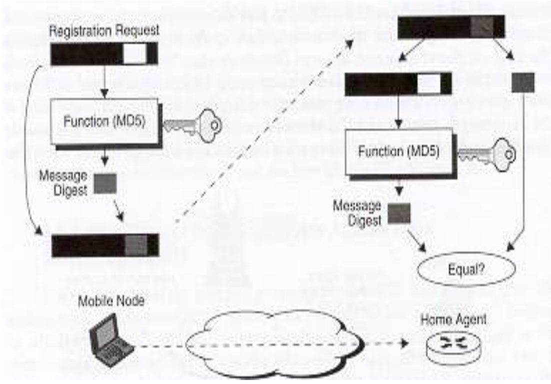


Figure 2. Function of MDS

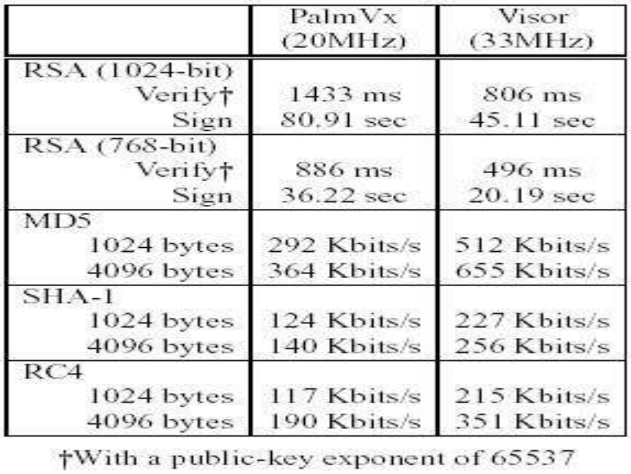
Let us consider a scenario, where Alice wants to send a message to Bob. Alice encrypts the message M using Bob's public key Pbob, which is exchanged before the session started. At Bob's side, this encrypted message is decrypted using Bob's private key Sbob, which is known only to Bob. Another function in public-key cryptosystem is the use of digital signatures. In this process, if Bob wants to send a message to Alice, he first signs the message M with his private key Sbob to obtain a digital signature S= [h (M) Sbob] of M, where h ( ) is one-way hash function. Here, hash functions like MD5 and SHA are used which accepts a variable size message and outputs a fixed sized representation h (M) of M. Alice decrypts this encrypted message by using Bob's public key. One of the widely used public-key cryptosystem is the RSA public-key cryptosystem proposed by Rivest, Shamir, and Adleman (RSA). This is a variant of RSA, where the public key is the modulus N, which is a product of two large primes. MSR requires only one modular multiplication for computing the encryption keys, and because of its low computational cost, is preferred over RSA.

7.1 Protocols based on Symmetric-Key Encryption

7.1.1 Encryption using Symmetric-key function

Performance

The certificate-based security protocol is considered to be more secure than symmetric key protocol in terms of key management. Because of its computational complexity, public-key cryptosystem is considered to be a burden on a mobile user with limited resources. Instead, a MSR with RSA system and low component can be used for mobile users. The results are as follows: the bulk encryption and authentication algorithms are adequately fast on Palm's CPU. On a 20MHz chip (found in Palm Vx, Palm IIIc, etc.) RC4, MD5, and SHA all run at over 100Kbits/s. When measuring SSL Handshake Latency, a typical key with size of 68 or 1024 bits using RSA takes 0.5-1.5 seconds on a 20MHz Palm CPU. The table shown below gives the performance of KSSL cryptographic primitives on PDAs.



	PalmVx (20MHz)	Visor (33MHz)
RSA (1024-bit)		
Verify†	1433 ms	806 ms
Sign	80.91 sec	45.11 sec
RSA (768-bit)		
Verify†	886 ms	496 ms
Sign	36.22 sec	20.19 sec
MD5		
1024 bytes	292 Kbits/s	512 Kbits/s
4096 bytes	364 Kbits/s	655 Kbits/s
SHA-1		
1024 bytes	124 Kbits/s	227 Kbits/s
4096 bytes	140 Kbits/s	256 Kbits/s
RC4		
1024 bytes	117 Kbits/s	215 Kbits/s
4096 bytes	190 Kbits/s	351 Kbits/s

†With a public-key exponent of 65537

7.1.2 Encryption using Diffie-Hellman Key Exchange Diffie-Hellman key exchange is another protocol that is used in Cellular Digital Packet Data (CDPD). This method takes advantage of the ease with which exponentials can be computed in a Galois field GF (q), where q is a prime of elements. As mentioned in paper [1], if y= _X mod q, for 1 < X < q-1, where _ is a fixed primitive element of GF (q), then X= log_ y mod q is referred to as the discrete logarithm of y to the base _over GF (q). Consider a scenario, where Alice and Bob want to communicate. Here, Alice selects a random number Xa between 1 and q-1, which it keeps as a secret and sends Ya=_X a mod q to Bob. Similarly, Bob chooses a random number Xb and sends Yb=_X b mod q to Alice. Once the two entities receive the messages, they compute Ks = _X, the security of this system is based on the difficulty of taking the discrete logarithm. The home networks, in visiting network VN (A) and VN (B) respectively. Initially, both, the mobile users and the visiting network authenticate each other thereby sharing a common session key using the Diffie-Hellman key exchange mechanism.

7.2 WLAN Basic Security Mechanisms

The IEEE 802.11b standard identifies several security services such as encryption and authentication to provide a secure operating environment and to make the wireless traffic as secure as wired traffic. In the IEEE 802.11b standard, these services are provided largely by the WEP (Wired Equivalent Privacy) protocol to protect link-level data during wireless transmission between clients and APs.

SSID: Network access control can be implemented using an SSID associated with an AP or group of APs. Each AP is programmed with an SSID corresponding to a specific wireless LAN. To access this network, client computersmust be configured with the correct SSID. Typically, a client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

7.3 Advanced WLAN Security Mechanisms WEP2: As an interim improved solution to the many flaws of WEP, the TGI Working Group of the IEEE proposed WEP2. Unfortunately, similar to major problems with WEP, WEP2 is not an ideal solution. The main improvement of WEP2 is to increase the IV key space to 128 bits, but it fails to prevent IV replay and still permits IV key reuse.

7.4 Virtual Private Networking (VPN): To further address the concerns with WEP security, many organizations adopt the virtual private network (VPN) technology. The VPN approach has a number of advantages. Firstly, it is scalable to a large number of 802.11 clients and has low administration requirements for the IEEE 802.11 APs and clients. Secondly, the VPN servers can be centrally administered and the traffic to the internal network is isolated until VPN authentication is performed. Another drawback in the VPN solution is the lack of support for multicasting, which is a technique used to deliver data efficiently in real time from one source to many users over a network. Multicasting is useful for streaming audio and video applications such as press conferences and training classes. Also, a minor issue of VPNs is that roaming between wireless networks is not completely transparent. Users receive a logon dialog when roaming between VPN servers on a network or when the client system resumes from standby mode. Some VPN solutions address this issue by providing the ability to “autore- connect” to the VPN.

IEEE 802.11i Robust Security Network (RSN) standard: To help overcome this security gap in wireless networks, the IEEE 802.11 working group instituted Task Group (802.11i) has proposed significant modifications to the existing IEEE 802.11 standard as a long-term solution for security, called Robust Security Network (RSN). An interim draft of IEEE 802.11i is now available, known as Wi-Fi Protected Access

(WPA).TKIP uses RC4, the same encryption algorithm as WEP to make it updateable from WEP, but it extends the IV from 24-bit to 48-bit in order to defend against the existing cryptographic attacks against WEP. Moreover, TKIP implements 128-bit encryption key to address the short-key.

CONCLUSION

Mobile computing is an important, evolving technology. It enables mobile personnel to effectively communicate and interact with the fixed organizational information system while remaining unconstrained by physical location With developments of latest technologies. It is expected that after Some years a number of mobile users will going to use cloud computing on their mobile devices. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality, access control as well as integrity to mobile users. Here in this paper we have in term identified some of the challenging Problems, applications of mobile computing along with few of the characteristics of Mobile computing.

REFERENCES

[1] T. Imielinski and B. R. Badrinath, "Mobile wireless computing: Solutions and challenges in data management," Technical Report DCS -TR-296/WINLAB-TR-49, Department of Computer Science, Rutgers University, NJ, 1992. \

[2] D. Brown, "Security planning for personal communications," in Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 107-111, ACM Press, 1993.

[3] M. J. Beller, L.-F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," IEEE Journal on Selected Areas in Communications, vol. 11, no. 6, pp, 821-829, 1993.

[4] W. van den Broek and E. Buitenwerf, "Distributed databases for third generation mobile systems," in Proceedings of the International Council for Computer Communication Intelligent Networks Conference (P. W. Bayliss, ed.), (Tampa, Florida), pp. 333-347, lOS Press, 1992.

[5] W. Itani, A. Kayssi, A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing,” in: Proc. Int. Conference on Energy Aware Computing, ICEAC ’10, Cairo, Egypt, Dec. 2010.