RESEARCH ARTICLE OPEN ACCESS

ISSUES IN MOBILE CLOUD COMPUTING

J.Mary Ramya Poovizhi
Assistant Professor, Department Of Computer Science, Immaculate College for Women, Cuddalore

Abstract

The web computing infrastructure was enhanced by a rapid growth of mobile computing and applications. Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. This paper presents security challenges in mobile computing and some investigated problems are given here regarding the safety of mobile computing system, among the framework of the classes of quality, disconnections, information access modes and scale of operation. In distinction to previous work that concentrates on security in wireless communications, we tend to focus on the safety of intersections that are engineered upon the underlying wireless communication medium.

Keywords: Mobile networks, Mobile Computing, Mobile Devices, Mobile Communication & Security

1. Introduction

The rapidly expanding technology of cellular communication, wireless LANs, and satellite services will make information accessible anywhere and at any time. In the near future, tens of millions of people will carry a portable palmtop or laptop computer. Smaller units, often called personal digital assistants or personal communicators, will run on AA batteries and may have only a small memory; larger ones will be powerful laptop computers with large memories and powerful processors. Regardless of size, most mobile computers will be equipped with a wireless connection to the fixed part of the network, and, perhaps, to other mobile computers. The resulting computing environment, which is often referred to as mobile or nomadic computing, no longer requires users to maintain a fixed and universally known position in the network and enables almost unrestricted mobility. Mobility and portability will create an entire new class of applications and, possibly, new massive markets combining personal computing and consumer electronics.

Researchers during this new field imagine that mobile computing units, such as today's laptops and palmtops, within the future are going to be human activity with one another via wireless networks, while providing place simplicity to the user. This vision of simplicity is carried-over from the actual fact that in distributed computing, the user is ignorant of the remote physical place of the resources that square measure getting used by the distributed computer system. The application scale of mobile devices is growing day by day which creates new challenges for information and security. Therefore how to care for the security of information and applications about mobile devices becomes a demanding problem. The expansion of mobile computing network is leading to latest security challenges.

2. Methodology

The selection criteria throughout that we evaluated study sources relies on the analysis expertise of the authors and to pick out these sources we have thought of sure limitation: studies enclosed within the selected sources should be associated with our downside and these sources should be web-available. The varied protocols for mobile ad-hoc networks are on the market. The Table-driven routing protocols plan to maintain consistent, up-to-date routing data from every node to each alternative node within the network. Source-Initiated on-demand routing creates route only if desired by the supply node. Once a node needs a route to a destination, it initiates a route discovery method among the network. Another step within the search method is performed by looking the connected work space of the chosen papers to boost the review efficiency by confirming that no useful reference is did not notice throughout the explore method. Once the sources had been outlined, it becomes necessary to explain the method and therefore the criteria for study choice and analysis.

3. Mobility and Protection

The fact that each user and therefore the knowledge that they carry became a mobile element in computing has in itself introduced a group of security issues completely different to it in traditional computing. Within the traditional case of mounted (non-mobile) computing physical protection may simply be afforded by creating a computer and information system physically isolated from the opposite parts within the setting.

In such a configuration it had been doable to form the system independent, without any got to communicate with the external world. More modern firewall techniques may also be applied to achieve an equivalent result. In mobile computing this manner of isolation and independence is troublesome to realize due the comparatively restricted resources obtainable to a mobile unit, thereby necessitating it to speak with the mobile support station. The quality of users and also the knowledge that they carry introduces security issues from the purpose of read of the existence and site of a user (which is deemed to be knowledge in themselves.) and also the secrecy and authenticity of the info changed between users and between a user and a set host. Additional specifically, a user on a mobile wireless network could prefer to have the knowledge regarding his or her existence treated as individual confidential. That is a user can like better to stay anonymous to the bulk of different users on the network, with the exception of a choose variety with whom the user usually interacts. This downside of user obscurity in mobile computing is expounded to a tougher downside of the trust level afforded by every node within the wireless network and therefore the drawback of the safety of location knowledge regarding a user once the placement knowledge is hold on or transferred between nodes because the user moves during an unsettled fashion. These nodes should give some assurance to the user concerning his or her obscurity, freelance of the differing levels of trust which will exist for every node. This demand is of specific importance within the case of a user that crosses between two zones that are beneath two nodes severally, every having a distinct trust level. Equally, necessary is that the secure transfer knowledge data between databases at nodes that hold location data and different information or parameters within the user profile. Here all traffic internal to the network and clear to the unsettled user should be maintained secure and authentic.

4. SECURITY ISSUES OF MOBILE COMPUTING

5.

The mobile computing is the communication between computing devices without a physical connection between them through wireless networks, which mean there are some of new mobile security issues that are originated from wireless security issues. The security issues and threats of mobile computing can be divided into two categories: security issues that related to transmission of information over wireless networks, and the issues that related to information and data residing on mobile devices.

5.1 Security problems in Mobile Devices

Mobile devices should be serious thought as a result of issue of security act as associate degree obstacle within the development of mobile services. Each security issue must be addressed at the terribly beginning of the service development method. The most mobile security threats for the developers of mobile services embody the complexness of technical solutions, prohibited repetition of programs and content and threats provided by the net.

5.2 Security problems in Mobile Network

Mobile networks are being driven by the requirement for providing network access to mobile or rootless devices. Although the need for wireless access to a network is clear, new issues are inherent within the wireless medium. Wireless but does not imply quality. There are wireless network during which each ends of communication are fastened like in wireless native loops. Therefore, a study of wireless knowledge networks has its own scope completely different from networking system normally.

5.3 Security problems in Mobile Communication

Wireless devices like mobile phones, PDAs and pagers square measure less secure than their wired counterparts. This can be as a result of information measure, memory and process capabilities. The opposite reason is that interruption of the information that is sends into the air. Establishing of secure wireless communicating is one among the key needs within the PCs. A number of the necessary problems which require attention in coming up with security theme for mobile communication square measure like autonomy of human activity entities, quality of the users and restriction of hardware.

6. Conclusion

In this study totally different articles and conferences were reviewed so as to produce an in depth read of security challenges in mobile devices, networks and communication. It is found that security of mobile devices could be a terribly serious issue. This area wants correct attention of the researchers to beat the protection problems during this domain. None of the work totally solves the total drawback attributable to the poor

interface of mobile devices, development in mobile networks and also the latest technologies in mobile communication. In future these mobile devices can access totally different networks. Therefore, the way to succeed new security challenges may be a possible question.

REFERENCES

[1]Mobile_Payments_Security_in_Proximity_Mobile_Payments
[2] Jon Oltsik-Addressing Mobile Device Securityand Management Requirementsin the Enterprise
[3] Sharad Kumar Verma, Dr. D.B. Ojha-An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks.
[4] Jun-Zhao Sun, Douglas Howie, Antti Koivisto, and Jaakko Sauvola-A Hierarchical Framework Model of Mobile Security.
[5] Swarnpreet Singh, Ritu Bagga,Devinder Singh, Tarun Jangwal -Architecture Of Mobile Application, Security issues And Services Involved In Mobile cloud Computing Environment
[6] Enaam Faihan Alotaibi and Adnan Mustafa AlBar -Mobile Computing Security: Issues and Requirements
[7] Dr. Pranav Patil -SECURITY ISSUES IN MOBILE CLOUD COMPUTING