MAJOR SECURITY CHALLENGES IN MOBILE COMPUTING

[1]A.Sony, [2]N.Venkateswaran, [3]R.Jegadeesan,[4]T.Rakesh, [5]CH.Divya Teja
[134]Students, [2,3]Associate Professor, Department of Computer Science and Engineering,
Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana-505001

Abstract: Mobile Computing is a specific form of human-computer interaction. In the present environment, the size of computing devices or machines are decreased with the power of computing, which is also used to develop computing devices like Laptops, Smartphones, Personal Digital Assistance which are useful and portable to carry from one place to other place and can access the information. Recently a lot of research is carried out, to improve the performance issues like handoffs security. The point that needs e considered which comes into picture when the communication channel is set up. In this, we can investigate some problems concerned with the security of mobile computing systems and focus on the protection of interactions which built upon the underlying wireless communications medium. Security issues should be identified to protect the physical devices and user's information. The objective and focus of the article is to highlight the security issues and to bring awareness to the users. Few conclusions and solutions presented in the future direction.

Keywords: Mobile Security, Mobile Computing, Wireless Communication

I.INTRODUCTION

Mobile Communication Security plays a significant role in mobile computing. Security is a significant issue for any device that computes when we access the internet and contains sensitive data. Security is compulsory in mobile computing devices such as mobile phones, computers, personal digital assistant(PDA's) due to mobility, wireless communication and portability. Mobile computing allows users to communicate with others with more flexibility and providing the data anywhere, anytime, with cellular phones[1]. He people enjoy various services brought by mobile computing. Mobile computing is becoming a global trend in today's world. Security mobile computing will pay by increasing attention. The Security issues to be deal with 3 properties: communication, mobility, and portability.

Security is essential for every network, but mobile computing presents more security issues than traditional systems. Secure mobile computing is critical in wireless network application development. The development of wireless technology has been increasing day-by-day which attracts ser, and that has become more popular[2]. The emergence of mobile computing has the latest version even though the technologies are updated. The security challenge is facing hackers who are ready to hack the user's information, and as the technology upgraded, users are now able to control security thefts happening by using various security protocols and methods on their device[4].

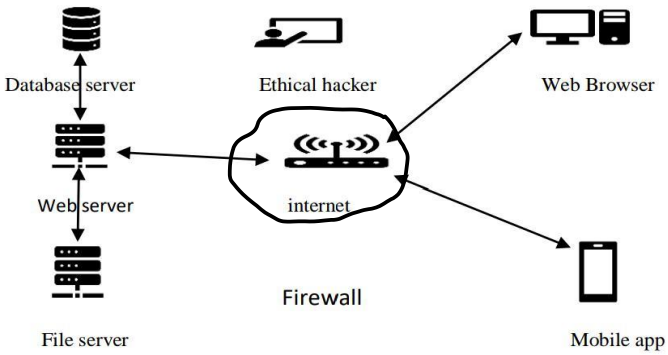

Fig :1: reflect issues in mobile computing

II. Major Security issues and Challenges:

Mobile Computing concept has its fair share of security concerns as any other technology due to this nomadic nature; it does not easy to observe the proper way of usage. People and users might have different intentions on how to utilize this privilege[4]

Inaccurate and Illegal practices such as hacking industrial tailing, copying, online fraud, and malicious deletion are some, but some of the problems experienced by mobile computing outsiders gain access to steal vital data from companies, which is a significant hindrance in rolling out mobile computing services[2].

The devices of mobile computing must be protected from security issues to provide security. Another major problem in mobile computing is credential verification. As other users share username and password, it poses a threat to security. The problem is to identify these theft's is very difficult and to eradicate issues with unauthorized access to content and information by hackers is also a different problem. All the companies don't want to lay open their secrets to hackers, and other intrudes, who will sell the valuable and confidential information to their competition.

We present more security issues due to the characteristics of wireless transmission and the demand for mobility and portability.

Mobility: Mobility means changing the position of connection to the network with being connected to the systems. If a mobile device user traveling from one cellular tower to another cellular tower that the mobile device can access the signal from the new mobile tower without breaking signal time. The medium and the network connectivity in mobile will not be lost, with mobility user can communicate anywhere, anytime, with any other users because mobility is a user dependent[14]. It is the technology powered, but business driven increasing is also a risk to the security of computer systems.

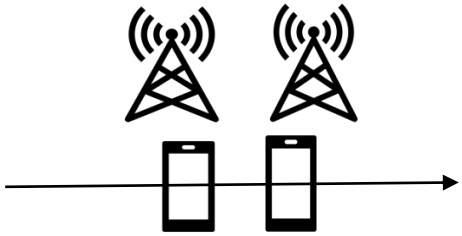

Fig :2 There is a loss of signal between two mobile towers

Portability: Portability means changing the position of connection to the network without being connected to the system. If the user traveling from one network to another network, there is a loss of network connectivity in the medium to access the internet[14]. With portability, the device can communicate online anywhere, anytime to the network. Because portability is a device dependent. Portability, Connectivity and Storage data capacity of mobile devices bring with them the threat of data leakage, data missed and the introduction of viruses to computing systems.

Fig 3: loss of network connectivity between two networks

Wireless Communication: It is a type of data communication and delivery of data through wireless. It is a form of communicating between two or more devices using a wireless signal. In Wireless communication information is transferred over a certain distance through devices like Bluetooth and using LAN's, WAN's to send data to others. These are facing challenges that unauthorized persons are tracing the signals to get the private information of users.

Fig 4: wireless communication

III. Security Requirements:

A functional security requirement is something that describes functional behavior that enforces security. It can be directly tested and observed. Conditions that have things to do with access control, data integrity, authentication, and wrong password block outs fall under functional. The following are fundamental goals of mobile security computing:

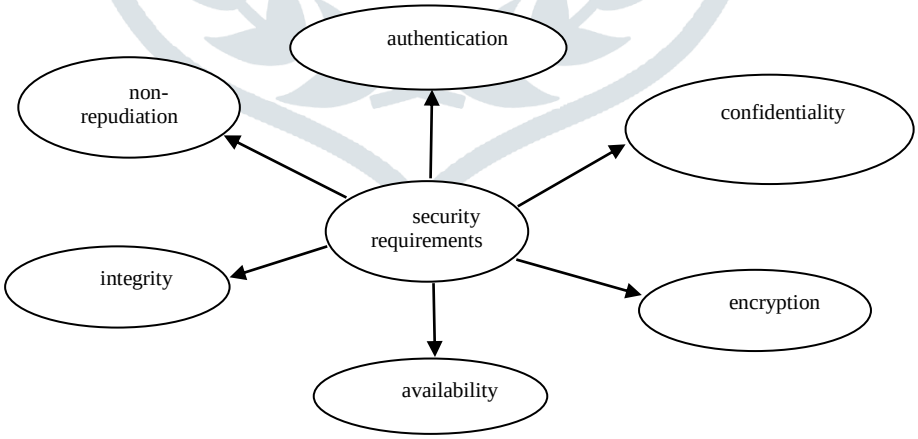

fig:5 security goals

1. **Authentication:** Authentication is nothing but access rights of the individual. It is used to authorize the mobile device verification of users identifies. This authentication includes logging into the security locations in which we enter usernames and passwords. Some passwords are non-text which provides for symbols or images, one-time password through messages. Which are comes under the methods of authentication [9]? Security environment, authentication is distinct from authorization, which is the processing of giving individuals access to system objects based on their identity. For example, mobile devices have fingerprint sensors, face recognition security system for avoiding unauthorized users.

2. **Confidentiality:** Confidentiality in the system only for authorized users can access the data. It is used to protect the information from unauthorized users and keep the data more secure when the data in motion the authorized users using a LAN network. In the way the data will be reliable no other persons can access[13]. While using the WAN network, the data may steal by unauthorized persons. The people who are authorized to do so can access the data. It is mandatory that information is available to the authorized user only.

3. Encryption: It is one of the process of converting the message from readable format to non-readable format. It is used on the internet to protect for user information available in the server. Encryption will be primarily in passwords, here we enter the text, and it will e converted into ciphertext. Encryption plays a significant role in payment transactions and personal information from unauthorized users. Encryption is used to protect sensitive data stored in computer, server and mobile devices[8]. The conversion of data into ciphertext format. It is the most effective way to achieve data security. Otherwise the process of converting data into the system, mainly to prevent from unauthorized users.

4. **Availability:** The resources are available for the authorized users is called availability. Availability of data refers to assuring that authorized users can access the data when necessary. Information only has value if the right user can access it at the right times[3]. The authorized user access with the resource is called a valid user. The funds are data, software, hardware and memory are available for the authorized user. The availability of the funds will reduce due to the "denial of service" attack. Access to content has become a very common attack now-a-day.

5. **Integrity:** If we send any message from sender to receiver, when the word is transferring to the receiver there is no change in the medium until receiver did not receive the news there is no change in the message bits in the medium. Sometimes in the medium due to involving of third-party person there is a chance of changing the bits or bytes in the message, Integrity is when we send the data to the receiver that should not be changed until the third-party person enter[8].

6. **Non-Repudiation:** Non-Repudiation is the assurance that someone cannot deny something. It refers to the ability to ensure that communication cannot deny the authenticity of that the sending of a message that they originated from denying [3]. Non-Repudiation guaranty that the message transmission between sender and receiver by digital signature and encryption. It is used for digital contracts and emails messages. Thus, nonrepudiation protects the receiver and sender when the receiver denies the receiving an email. Without nonrepudiation, information security would be not perfect.

IV. Security Goals:

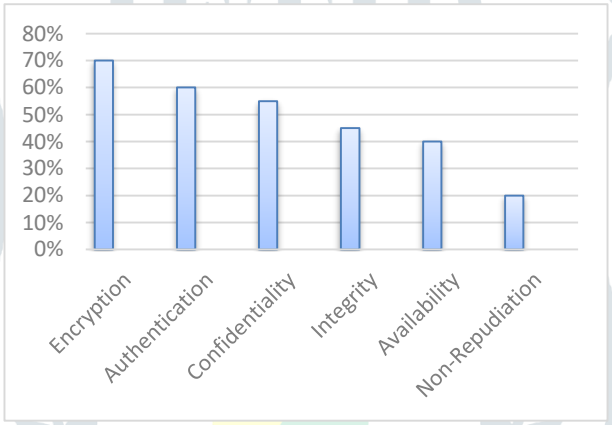

fig: bar chart representing security goals

1. Encryption gives more security than any other requirements. Because encryption changes the text message into an unreadable format which cannot be authenticated by the unauthorized person. So, the encryption gives more secure to sensitive data. Data will be encrypted and exchanged between the client and server like credit card numbers will be sent through the internet with less risk.
2. Authentication is also the requirement used for mobile device security. By authentication, only the user can authorize the device. In authentication, the user has to prove its identity to the server or client.
3. Confidentiality refers to protect data from being accessed by unauthorized users. Confidentiality will use in bank records. You should be able to obtain bank records, of course, bank employees who are helping you with a transaction should be able to access them but not others.
4. Integrity refers to ensure the authentication information is not altered, and it should be genuine information — integrity used in web sites. The failure of integrity is when the user tries to connect to the website, and an attacker between the user and the website deviate the traffic to a different site.
5. Availability use, when the attacker is not able to compromise with confidentiality and integrity, and they may try to execute attacks that would bring the server down and making the website unavailable to users.
6. Non-Repudiation will use for security requirements. It is used to protect the data transfer between the sender and the receiver that the receiver does not allow the messages. Non-Repudiation will use in digital signatures. It has fewer security requirements compare to the encryption.

V.Proposed Deployment:

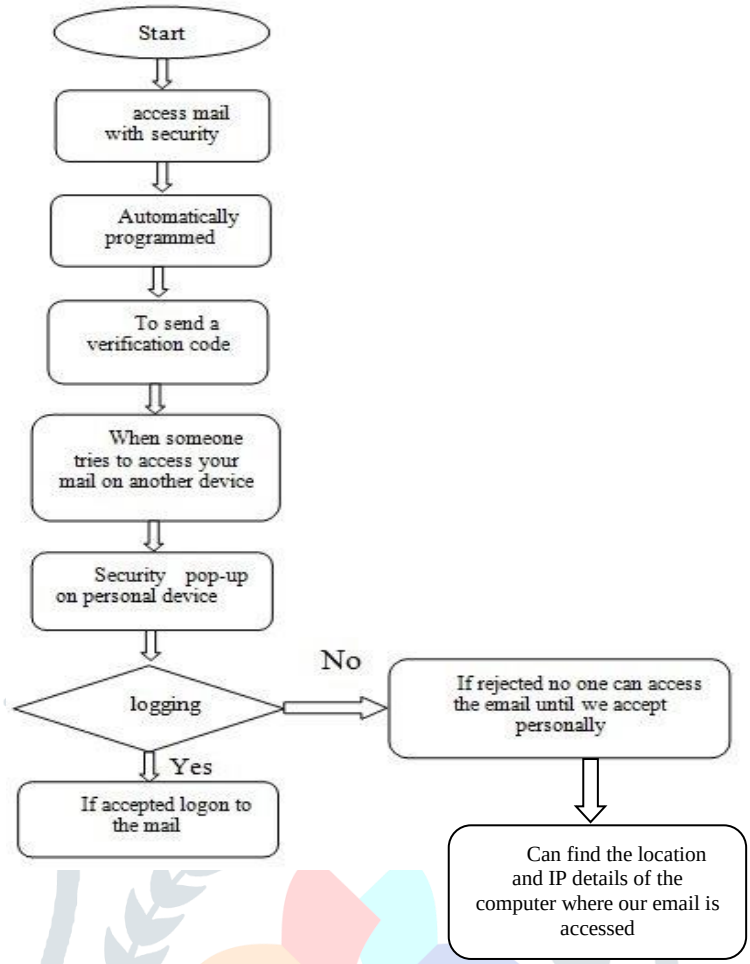

fig: flow chart to access mail permissions

In the day-to-day, the number of the data network, digital applications, as well as internet and mobile users, are growing. So do the chances of security explanation and Cyber-crime. Even a small mistake in security data or bad social networking can prove to be extremely dangerous. If email accounts are not properly secured, it makes it easier for hackers or unauthorized users to spread viruses or social engineered attacks that are designed to steal data.

For Example, in the diagram(fig:(a)), if any authorized person tries to access your email without our permission where all the confidential information will store, we have the security protocol which is automatically programmed to protect and maintain the confidentiality. Here we get a security pop-up on our device once our mobile number and device are synchronous to our email. Trying to log on to other equipment and if once we accept that pop-up message, we will be able to access the email and if we are not trying to locate it we can reject it. We get the location and device details on which the unauthorized user tried to log on to our email, with which we can track the hacker or unauthorized user.

To protect mobile devices from threats:

Mobile device needs and users are increasing day-by-day; the dangers encountered by mobile users are also growing. Here we provide some instructions to keep users data stored in mobile device and mobile device securely. The instructions are as follows:

- Verify that the data stored in the mobile devices are encrypted[3].
- Check that the data backup of mobile devices stored in secondary memory.
- Make sure that the data stored in secondary storage devices like hard disk, solid state drive, USB flash drive are encrypted.
- Ensure that Anti-Virus software installed in your device.
- Make sure that Bluetooth, Wi-Fi is turned off or not[3].
- Check whether the firewall is established or not in the mobile device which is a network security system that controls network traffic based on security rules[3].
- Ensure that the mobile device encoded with a highly secured password.
- Immediately inform to the Superior if the mobile device s stolen.
- Ensure that Mobile device is arranged with a power-up process to prevent from unauthorized users access if stolen.

VI. Conclusion

The objective and focus of the paper is, to describe the security issues and challenges of mobile devices, possible solutions and requirements discussed, we are providing some information based on awareness of security threats to authorized users and they should protect their data from unauthorized users. In this rapid technology environment data stolen, cyber-related risks are a common issue. This type of attackers is to take confidential information they have a variety of tools that can harm your mobile device opening the email attachments that carry the virus, downloading a dangerous program are ways to be data stolen, and users should be attentive regarding their information providing to others.

References

[1] Sunil Lalwani, "Mobility for a dynamic workforce," The Hindu, Dec. 9, 2012.
[2] "The Impact of Mobile Devices on Information Security: A Survey of IT Professionals," Dimensional Research | January 2012. www.dimensionalresearch.com.
[3] International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017.
[4] en.wikipedia.org/wiki/Mobile computing.
[5] www.tutorialspoint.com/mobile_computing/mobile_computing_security_issues.html.
[6] Collin Richard Mulliner "security of smart phones," Master's Thesis, University of California, Santa Barbara, July 2016.
[7]D.P.Agarwal and Q.A.Zeng, Introduction to wireless and mobile systems, Brooks/Cole Publisher, 2002.
[8]A. Gangula, S.Ansari, and M.Gondhalekar, "Survey on mobile computing security," in Proc. 2013 European IEEE, Conference on Modelling Symposium, November 2013.
[9] "Security Issues in Mobile Computing," Srikant Pullela, Department of Computer Science University of Texas at Arlington.
[10] I. Mavridis and G. Pangalos, "Security issues in a mobile computing paradigm," Springer. E, vol. 3, p. 61, August 1997.
[11] M.Satyanarayanan, pervasive computing: vision and challenges, 2001.
[12]International Journal of Review and Research in Applied Sciences and Engineering, Vol.7 No.1 2015
[13] COMPUSOFT, An international journal of advanced computer technology, 3 (2), February-2014 (Volume-III, Issue-II)
[14] M. Satyanarayanan, "Fundamentals Challenges in Mobile Computing," in ACM Symposium on Principles of Distributed Computing, 1995.
[15].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[16]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[17]. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[18]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013)
"Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[19]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 "NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[20]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[21]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[22].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014
[23]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[24]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)
[25]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)
[26]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[27]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018
[28]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.
[29] International Conference on Advanced Computing (ICAC-2016), College of Computing Sciences and Information Technology (CCSIT), Teerthanker Mahaveer University, Moradabad.
[30] http://www.dauniv.ac.in/downloads/Mobilecomputing/MobileCompChap01L07_MobComputing.pdf.