Security Techniques for Counteracting Attacks in Mobile Database

Usman Ahmed, RasoolBukhsh, SehrishNasreen Muhammad Azeem AkbarFaisal Mehmood
usmanahmed@teachers.org,
rasoolbax.rb@gmail.com,sehrishch2894@gmail.com,azeem.akbar@ymail.com,faisalmehmood685@gmail.com

Abstract: The use of mobile devices has become very common and essential now a day. It's this popularity made these devices easy target for malicious code developers. And the ratio of these attacks is increasing day by day. Because of static environment the features of mobiles are specials and limited, for example frequent disconnections and movement in the user's location, these are the reasons which affect the security mechanism. It is the security mechanisms which have become the reason of delay for a user to access the data. Because of this delay changes has to make in access conditions. The contra effect of security and access mechanism cover these changes dynamically. In this article, efforts have been made to use different security mechanisms to establish access control dynamically.

I. INTRODUCTION

If you watch secret agent movies you will judge that officials are investigated at different points of exit and entrance to control the exposures of secrets. Now a days panama leaks is the biggest example of the lack of security in securing the information. In the panama papers almost 11.5m files are leaked from the database of Mossackfonseca through ICIJ (International consortium of Investigative Journalist). With the help of this example it is clear that we cannot assure the security of data just on the behalf of classification and entrusting the people. Therefore effective measures should be taken to secure the important information. Now a day with the help of portable devices everyone can easilytransfer the data from one place to another place. No doubt, this technology is very much effective but also harmful for the security of information. For example being an official of any organization it is very easy for someone to download the information into portable device and then handed over it to any person who can leak this information like a panama paper. As a result of this leakage your firm will lose its reputation in the market and nobody will trust upon your organization ultimately. To avoid these consequences continuous and dynamic access to information should be controlled. The DBMS is deeply affectedbecause of portable devices. In the remaining part of this article efforts will be done to discuss the limitations of mobility and their impacts on database management system. After this access control methods will be introduced those will guide us how to control these complications. Access control techniques have three parts: (1) identification and authentication (2) authorization and (3) audit.

II. LIMITATIONS OF PORTABLE DEVICES

No doubt the cellular companies are introducing new mobiles with lots of new apps with the everyday past but instead of this progress there are manylimitations in these mobile devices like power problems, small display problems, low band width problem and many others like these, a major problem which needs to discuss separately is the continuous disconnection. The reason of this connection may be the weak signal or hanging off the mobile devices or the shutting down of the mobile device. The robbery of the device is another major problem of mobile devices.

IJSER

III. LITERATURE REVIEW

The use of mobile has become very common even a lay man is also using this device freely. This device is used for different purposes like the receiving of data, the transfer of data etc. In an organization you are not allowed to share important information outside the organization. So there is a need to control user access on particular information. To control data in user's mobile; we use mobile agents and install these agents in user mobile. It is called Access control Agent (ACA). These agents work in two ways, first of all it restraints the user in treating his data, and if it sees any changes in the data, it blocks the user.it also controls the fake user to use the data illegally.Secondly it works to act upon the users 'requests. For the performance of this activity ACA has to develop an agent which is called ''Query Agent'' (QA) and transfers it to a ascertained destination. (Amin Sedaghati, 2010)

Mobile database has to face many security threats. If there are threats then the solutions of these threats must be possible. As a part of distributed system mobile database has to face a lot of security problemsIn the paper we deal with the security of mobile database on four fields. The first field is relating to the security of mobile device. The second field define the security of operating system in mobiles. Other two fields include the security of mobile device itself and security of networks. The security of any distributed system is based on authentication, identification and access control .if any of them will not properly work then security issues will arise. The first level in the security of mobile device is Authentication. It verifies the user. While identification verifies the identity of users. Password is the common method used for the authentication and the identification. But password is not enough for authentication and identification. Some users have started to use biometrics as a user's identity. The protection and the alteration of data is the key role of access control.(Parviz Ghorbanzadeh, 2010)

The identity and authentication are major source for the mobile users to secure their device database. The protection of access control process is essential, Encryption should be enhanced and backup must be considered necessary. To make sure the prevention of the illegal access to information there is a need for identity and authentication from the user. The access control need protection and ensures that there is no illegal access of data from unauthorized users. To make the database more secured there is need of dynamic security system. Only access control on data is not enough for security and privacy of data because mobile database stored very important data in it so there is need for encryption to prevent unauthorized access. First of all password should be set up. Separate passwords should be used at the different levels. Second mobile backup should be used for safety of database. (Wang et al., 2010)

Now days there is often use of biometric authentication for authorization and identification of user. This often used due to the many applications provide biometric mechanism for identity of user. Such as remote log-in to secured systems, securing

IJSER

mobile devices, cars, buildings, and terrorist monitoring applications. Hand Geometric is one of the physical methods that proved to be a good biometric for identifying the person. That is because it has multiple advantages over other biometric such as it is easy to use and small amount of data required for uniquely identify a person. But there is only small number of databases available for research and there is small number of users to use these applications. For this purpose there are two hand image databases, mobile hand image database (MOHI) and Webcam hand image database (WHI). These databases were designed to be used for different purposes, such as, identification of persons, authentication of persons, to distinguish between male and female and classification of people by age groups. (Hassanat et al., 2015)

There is need to enhance the security in better way. Threats on security of data are increasing day by day. So enhancement in security of database becomes necessary. For this purpose the security enhanced module are designed to improve the database security in better way. After testing the security enhanced module, it is realized that the security of database is enhanced. Illegal operations are interdicted and system response time is increased. By using the database optimization, safety of database and performance of database will increase.

Different types of security enhancement modules are given below:Security detect module, interaction module, access security checking module andmanagement module. (Wang et al., 2013)

The use of mobile in obtaining the information relating to health on internet is rapidly growing because of limited security arrangements mobile devices were easily attacked. In this article suggestions are provided that how to protect the devices from attackers. Distributed Denial of Service (DDoS) is the major threat in the internet. There are many challenges when it deals attacks in mobile nodes to their limited resources. When the security attacks are dealt in mobile nodes, many challenges arises. Our model prevent attack at the nodes. According to our point of view deniel of services attack can be controlled through Security Enforcement Component. The security enforcement component (SEC) provides secure communication and deals with the attacks on mobile devices. (Tupakula et al., 2013)

In this article the development in security of database, privacy levels of data, data mining for the security of cyber applications are defined. This paper provides directions for database security research. There is big problem to manage and analyze large amount of data by database researchers and developers, they should ensure privacy of data, security of data and provides safety from attacks on data which is going to be a big problem in future. There is a need to determine what technique should be there and how to apply them for securing and maintaining the privacy of data. There are different commercial products to secure and manage data in best way. There are different ways to precede it that are: First there is a need to keep up with technology development. Second, there is a challenge to imply the privacy techniques, and there is a need to improve the security models that

IJSER

should be useful for different types of data. (Thuraisingham., 2015)

IV. Methodology

A wired network is used to connect the different wireless networks in the data base system of a mobile. Several technologies like mobile phone networks, infrared etc. are main parts of wireless technology. This technology first read the data and then moves it to the user's device if the data is free from any malware. An agent who is called Access Control Agent is installed in the user device to control the data. Access Control Agent performs two functions. First of all, it controls how to treat the information it has a regular check on the data and update the permission if it finds any change in data. It also controls the data from any illegal and unauthorized used through any agent called query agent. Query agent received the information from the access level of user and delivered it to access control agent. Secondly local servers are used to deal with the incoming query agents and to check their access permission. There are several local servers which are connected with each other and also with the data base management system via fixed network. Every local server is controlled by an agent known as Local Server Agent.

A. Capability Lists

In this article efforts will be done to protect the data against any unauthorized use. For this purpose Capability Lists Access Control Model is preferably selected out of several access control techniques. It is used to store the access permission files as the information and data which is stored in these files is very important, therefore effort will be done to use different passwords at different levels. These passwords must be encrypted so only the authorized person can use, copy and remove the data if he needs.

B. Biometric technique

In the movies it is seen that important data are stored in safe or rooms locked with biometric if any unauthorized user try to steal the data an alarm is started and situation is controlled easily. In fact these scenes of movies are providing the proves that biometric system is more reliable security system. Biometric technique used two approaches for the security of data. First is enrollment and second is verification. In enrollment specific physiological information, "face scan, finger print, hand scan, eyes scan, DNA", and behavioral information, "Signature, Keystroke and voice", of the user are feed in the device. In the second approach, which is verification, reliable devices, like scanner are installed to compare the security check which was feed through enrollment approach for accessing the data.

C. Backup and Recovery Techniques

The data that saved in mobile database is very important, so the different backup methods should be used for the recovery of data. It will be useful in that case, if the system has been failed due to different reasons; data can be recovered again quickly.

V. Summary

IJSER

With the popularity of mobile devices the malicious code developers easily attack on these devices, so the access control mechanisms like authentication, access control, identification and authorization should apply to protect the devices from the unauthorized access and misuse of data. To protect the devices from unauthorized access biometric system is there that control the device from unauthorized users. In case of any failure in system, data can be recovered through backup and recovery mechanism.

REFRENCES

1. Ghorbanzadeh, P., A. Shaddeli, R. Malekzadeh and Z. Jahanbakhsh. 2010. A survey of mobile database security threats and solutions for it. IEEE.1-8.
2. Hassanat, A., M. Al-Awadi., E. Btoushand A. Al- Btoush. 2015. New mobile phone and webcam hand images databases for personal authentication and identification. Procedia Manufacturing. 3: 4060 – 4067.
3. Sedaghati, A. and A.B. Dastjerdi. 2010. Access control in mobile databases using mobile agents. IEEE. 1-4.
4. Thuraisingham, B. 2015. Database security: past, present and future. IEEE. 1-3.
5. Tupakula, U. and V. Varadharajan. 2013. Security Techniques for Counteracting Attacks in Mobile Healthcare Services. Procedia Computer Science. 21: 374-381.
6. Wang, P., L. Xing., X. Gu and C. Zhu. 2013. Design and implementation of security enhanced module in database. IEEE. 1-3.
7. Wang, H., D. Dang and S. Min. 2010. The analysis of the security strategy of embedded mobile database. IEEE. 1-3.

IJSER