Mobile Database: Security Issues and Research Areas

Nimish Joseph, Nitish Rawat, Rahna E

Dept. of Computer Science and Engineering,

National Institute of Technology, Calicut

Kerala, India

Abstract— The mobile database may encounter a series of safety problems from the mobile client, the wireless network, the loophole of itself, the attacks from hacker, viruses and so on, in the actual application process, while the data security of backend database is under threat. To ensure the safety of mobile database, the identity authentication must be consummated, the access-control mechanism should be strong, the database Encryption must be enhanced, the audit, backups, and recover must be taken into account, the mobile client authentication should be enhanced and the wireless transmission must be encrypted. We also review the state of progress in mobile databases and identify major research directions in this field.

Keywords-Embedded mobile database, the safety problems, the security issues, performance evaluation

I. INTRODUCTION

The mobile database refers to a distributed database which supports mobile computing environment. Due to the mobile database system is usually used in the PDA, trackside equipment, mobile phones and other embedded system, so it has been called the embedded mobile database system.

II. THE SECURITY PROBLEMS OF MOBILE DATABASE

Data security is a serious threat in the process of transactions because the mobile database is running in the open mobile environment. The safety problem it faces in this case is shown in figure 1.

A. Security Threats of Mobile Terminal

Mobile terminal is usually easy to carry, but also easy to lose and theft. So the attacker can obtain the terminal equipment for such as digital certificate and resources, unauthorized access enterprise internal network resources or destroy the data of mobile terminal.

B. The Wireless Communication Network Itself

It is a potential threat to the information security and personal security of the wireless network users, because wireless communication network communicates through an open channels.

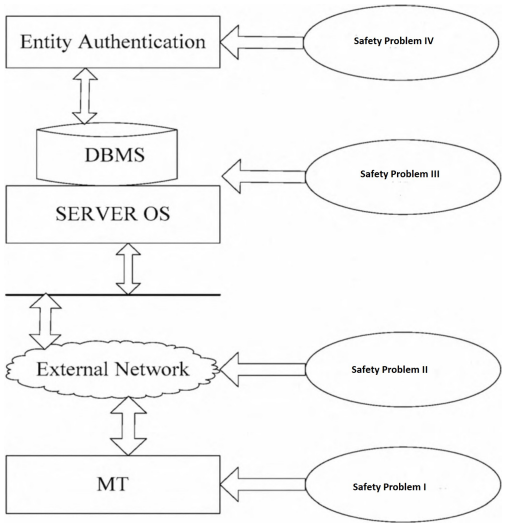

Figure I. Security problems that mobile database faced

C. The Security Vulnerabilities of Mobile Database System

First, database technology development to have certain restriction, there are many deficiencies, the repertoire of database system is arbitrary, which let the invaders easily to get the management authority of operating system, and it Userdirect threat the operating system security server.

D. From the Outside Factors of Database System

The hacker attacks, hackers may eavesdrop, fake, excessive and circuitous attack on the mobile database system, thus filch data or disrupt the normal operating system. And, the type of virus, which can make more mobile terminal equipment and backend database damage and attack. Finally, the information encryption and confidentiality of mobile database application system is not ready, distributed transaction and fault recovery is not comprehensive.

E. Lack of Effective Entity Authentication

Mobile clients cannot be trusted to confirm its authenticity of identity to server database. The user may eavesdrop the packet switching to use replay supply into the database server or interrupt the operation

III. THE SECURITY STRATEGY TO MOBILE DATABASE

To protect the mobile database security, we must prevent leak, change or damage data and should provide more reliable safety certification. The system safety model of mobile database can be consisted of the following:

A. Perfecting the Authentication Mechanism

It need for identity authentication, when mobile clients and service database operating synchronous in the mobile database system. **WPKI** (wireless public-key system) can effectively solve the problem of identity authentication database. Eg: RSA, Diffie Hellman.

B. Further Strengthen Storage Access Control

The access control needs protection data determine to grant and implement authority. Before users access the resources of mobile database, it should grant their visit corresponding system resources right. The grant and revoke command are comonly used, like:

```
GRANT privileges ON object TO users [WITH GRANT OPTION]
```

C. Strengthen the Encryption of Data

To enhance privacy, the mobile database system stored data need to be encrypted to prevent leakage. Firstly it needs to set a password encryption, by setting different levels of password. Secondly, the storage of data must be done after encryption using different encryption methods such as the use of elliptic curve cryptography (ECC). It increases the database data security, and now there are no effective methods of attack break.

D. Taking the Audit trail and Attack Detection into Account

The authentication and access control can effectively guarantee the security of the system, but there will always be system security vulnerabilities, the audit trail and attack detection is very important. The attack detection system detects the internal or external attacker attempts based on audit data, to track down the responsible person,

E. *To Improve the Backup and Recovery Capabilities of Mobile Database*

The tape backup, hot backup, manual backup methods have to be used for safety backup of the database to ensure that the system has been destroyed for various reasons, can be quickly put into use again.

F. The Security of Wireless Communication Path

Bluetooth technology, use the authentication mechanism for system encryption to ensure the identity of communications identified. Effective use of data encryption technology to encrypt the data packet encryption and data encryption in the middle of the process, prevent the system from being attacked or data theft. The Mobile IP technology uses a tunneling technology, data encryption, authentication and many other safety measures to ensure reliable communication.

IV. OPEN RESEARCH TOPICS

There has been relatively little research on mobile database

systems in which not only the vehicles moving, but also the environment is mobile. It includes systems involving tracking (or planning) vehicle movements in continuous domains (at sea, in the air, cross country motion of SUVs (or tanks), etc.) in which the environment is also mobile. Such systems will effectively need to integrate mobile databases with spatio-temporal databases.

Today most mobile databases assume that data values (vehicle locations, road segment transit times, road network connectivity) are known with certainty. We need systems which can cope with uncertain data concerning vehicle locations, road delays, connectivity, location and direction of weather systems (e.g., hurricanes).

Another issue is about energy consumption. Because of the energy limitation of battery-powered clients, the mobile database community has been the first database community that addressed the energy consumption issue.

Last but not least is the topic of performance evaluation. Like in many database research areas, works in mobile databases often use synthetic data or a small set of real data to evaluate their performance.

V. CONCLUSION

With the continuous promotion of mobile computing technology and use of mobile database technology, the data security is a concern. So it's important to continue to explore the security issues of database system in the mobile environment. We will need to develop mobile database systems which can cope with millions of mobile clients and which cope with mobility in road networks, 2D, 2.5D, 3D settings, and which can cope with uncertain data, and mobility of both vehicles (persons) and the environment. We will need to also extend the systems to accommodate sensing applications where data streams characteristics are taken into account.

ACKNOWLEDGMENT

We express our sincere thanks to Dr. S D Madhu Kumar, Associate Professor of our department for his kind and wholehearted support in bringing out this paper. We extend our thanks to the God almighty who has been the backbone-support throughout.

REFERENCES

[1] Huaixiang Wang, DeyuDang and Shi Min, “The Analysis of the Security Strategy of Embedded Mobile Database”

[2] Le Gruenwald , Frank Olken , “Mobile Database Research: What Is To Be Done?”

[3] “Mobile Databases: a selection of Open Issues and Research Directions”, Author manuscript, published in “ACM SIGMOD Record 33, 2 (2004) 78-83”.