Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1174 – 1182

RESEARCH ARTICLE

Mobile Database Review and Security Aspects

Bhagat.A.R[1], Prof. Bhagat.V.B[2]

Dept. of Computer Science, P.R.P.C.E.T, Amravati, MH, India
Dept. of Computer Science, P.R.P.C.E.T, Amravati, MH, India

ashbhagat1990@gmail.com; mat.vaishali2@gmail.com

***Abstract*—**

This article show different introduction to mobile database and its threat along with their security that may be occurs for mobile database in the real world and gives possible solution to eliminate them and this work, a case study of a secure mobile database application. In particular, we design, implement and evaluate a mobile database. The importance of databases in modern businesses and governmental institutions is huge and still growing. Many mission-critical applications and business processes rely on databases. These databases contain data of different degree of importance and confidentiality, and are accessed by a wide variety of users. Integrity violations for a database can have serious impact on business processes; disclosure of confidential data
in some cases has the same effect. Traditional database security provides techniques and strategies to handle such problems with respect to database servers in a non-mobile context. We identify a set of security issues and apply appropriate techniques to satisfy the corresponding security requirements.

Key Terms- Replication, Security, Mobile Databases, Mobile Devices

I. INTRODUCTION

A Mobile devices are gradually becoming commonplace. The computational and networking power of mobile devices is constantly increasing and new technologies are integrated into them to support new functionalities and services. On the other hand, the field of databases and more generally data management is also expanded with new services and applications. Several modern database management systems support small-footprint databases that can be executed on mobile devices and admit disconnected computing and synchronization with a central database. We call an application that comprises a server with a central database and a number of autonomous mobile clients with replicated parts of the database a mobile database application.

One of the most important issues of modern computing systems is the pro-vision of sufficient security and privacy guarantees for the user data. Security issues of mobile devices are discussed in recent works like [7]. In the field of databases and database management systems, security is a well-studied subject. See for example [8] and the related chapters in [6, 3, 10]. More recently, issues about privacy in databases are discussed for example in [1]. However in the case of a mobile database application there are additional security challenges due to the distributed nature of the application and the hardware constraints of mobile devices. Achieving a sufficient level of security for such a platform is an important problem which has to be addressed. For example, data privacy and confidentiality is identified in [2] as one of the critical open issues and research directions in mobile databases.

Now, Mobile Devices database Management commonly called as Mobile Database' is either a stationary database that can be connected to by a mobile computing device - such as smart phones or PDAs over

mobile network, or a database which is actually carried by the mobile device. This could be a list of contacts, price information, distance travelled, or any other information.[1] Many applications require the ability to download information from an information repository and operate on this information even when out of range or disconnected. An example of this is your contacts and calendar on the phone. In this scenario, a user would require access to update information from files in the home directories on a server or customer records from a database. This type of access and work load generated by such users is different from the traditional workloads seen in client–server systems of today.

A mobile database is a database that can be connected to by a mobile computing device over a mobile network. The client and server have wireless connections. A cache is maintained to hold frequent data and transactions so that they are not lost due to connection failure. A database is a structured way to organize information. This could be a list of contacts, price information or distance travelled.
The use of laptops, mobiles and PDAs is increasing and likely to increase in the future with more and more applications residing in the mobile systems

For many businesses applications are going mobile that means using enterprise data in a mobile context, thus using a mobile DBMS. With these new developments the business data of an enterprise can be made available to an even larger number of users and a wider range of applications than before.

To work on business data anytime and anywhere is the major goal pursued by developing mobility support in database context. The confidentiality of mission- critical data must be ensured, even though most mobile devices do not provide a secure environment for storage of such data. Security requirements that apply to a central company database should apply similarly and in an appropriate manner to the parts of the database replicated on mobile devices in the field. A mobile database security infrastructure is needed to accomplish this goal. When developing such an infrastructure we can benefit from the results of traditional database security work. But we also need to adapt the existing techniques and strategies to the mobile context, and we need to develop new ones that attack certain issues specific to use of database systems in a mobile environment.

A. Concepts and the mobile platform

In this work, we define a mobile database as a small-footprint database that is installed on a mobile device. Most commonly the local database is a replica of a part of a central database that is installed at a server computer.

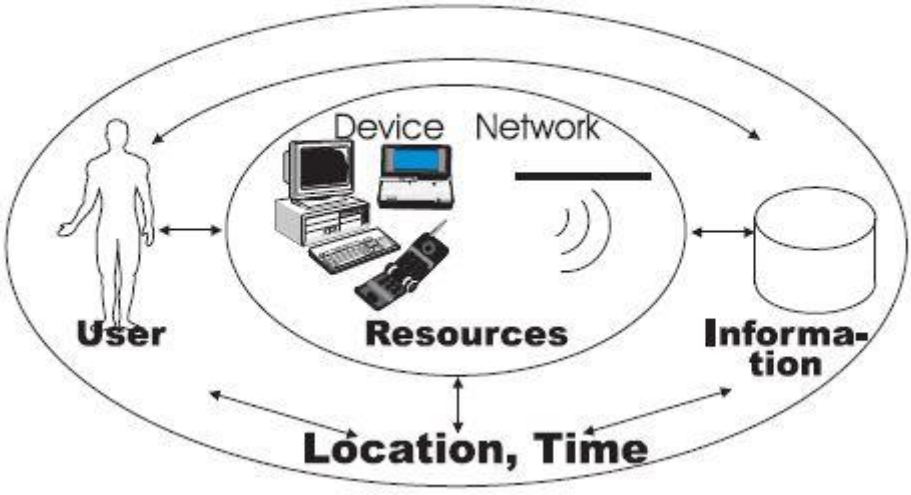

fig. General Mobile Scenario

Name	Developer	Type	Description
SQL Anywhere	Sybase iAnywhere	Relational	Embedded/portable database, can synchronize with stationary database
DB2 Everyplace	IBM	Relational	Portable, can synchronize with stationary database
IBM Mobile Database	IBM	Relational	Portable/embedded small-footprint version of solidDB server
SQL Server Compact	Microsoft	Relational	Small-footprint embedded/portable database for Microsoft Windows mobile devices and desktops, supports synchronization with Microsoft SQL Server
SQL Server Express	Microsoft	Relational	Embedded database, free download
Oracle Database Lite	Oracle Corporation		Portable, can synchronize with stationary database
SQLite	D. Richard Hipp	C programming library	Public domain
SQLBase	Gupta Technologies LLC of Redwood Shores, California		
Sparksee 5 mobile (http://www.sparsity-technologies.com#sparksee)	Sparsity Technologies (http://www.sparsity-technologies.com)	Graph database	Small-footprint embedded/portable database for Android, iOS and BB10. It allows traversals of nodes, minimum distance computations, community search, etc.

B. Motivation

In a mobile database application a part or a replica of the database is locally installed on the mobile device. This is a significant difference compared to a conventional client-server application where all data is centrally stored in a database server. The approach with a mobile database provides the necessary autonomy to the mobile device to work independently from the central database. The client application can work with the mobile database asynchronously, and needs to connect to the central database only when it is necessary to synchronize. This approach has several advantages compared to a conventional approach where the clients do not use local storage:

– Flexibility and Reliability: Asynchronous operation makes the application more flexible and tolerant to network failures.

– Efficiency: Except the synchronization steps, for all other operations the client has immediate access to the data since it is locally stored on the mobile device.

– Enhanced security: Disconnected computing reduces the total time that the mobile device is exposed to potential attacks over the network.

– Energy efficiency: The mobile device has to operate its network system, hardware and software, only during the synchronization operations.

– Reduced fees for network usage: This holds in the case where the usage of the communication link is charged. If the network link up-time is charged.

II. LITERATURE REVIEW

The process of the research into complex data basically concerned with the revealing of hidden patterns.

A. Review

The introduction provided evidence the demand for both mobile database access and secure database access, within healthcare, are increasing together. At their intersection is the need for secure mobile databases.

Yet, the research field for secure mobile database design is newly emerging, and as such, is disjointed. What is occurring is that research done in secure data access models, and separate research done in optimal mobile database design, are gradually coming together into emerging research on secure mobile database design.

Thinking of the letter 'Y' provides a useful visual (see Figure 1). On the upper left branch is the work done on secure database design. On the upper right branch is the work done on mobile database design. The lower central portion of the letter represents their emerging applications. He goes on to further discuss newly emerging access control schemes, such as role-based access control (RBAC) and the use of metadata intermediation, but notes these models are neither fully developed nor tested. "The DAC and MAC models lack capabilities needed to support security requirements of emerging enterprises and Web-based applications…Newer models have the potential to support emerging applications. However, these security models are yet to be fully developed and assessed."

Augmenting the traditional entity relationship (ER) database schema to explicitly address security concerns is the central focus in both the Pernul (1998) and Myers(2000) papers. Commonly, entity relationship diagrams are used to provide considerable detail about a database's entities, attributes, and relationships. Data access controls are rarely, if ever, acknowledged. Pernul (1998) takes the entities present in a database and subjects them to varying security classifications ranging from unsecure (U) to total security (TS). These hybridized entities (original plus security classification) are then re-modeled in the ER diagram. This application of security classifications at the entity level represents a limited mandatory access control (MAC) approach. Pernul's argument for adding security classification to the most basic level of database modeling (i.e., entity classification and modeling) is quite compelling, although limited. He does not, for example, apply security classification to data users as well.

Myers (2000) takes the approach that decentralized databases

To summarize, a review of the literature reveals that the secure mobile database design is a developing research field. Moreover, its "parent" research fields (secure database design and mobile database design) continue to evolve as well. More in-depth understanding is occurring on how to craft more stringent and usable security methods while, at the same time, knowledge grows on how to design database that work more effectively in the mobile setting. Secure mobile database design is the joining of these disparate and growing fields.

III. PROPOSED WORK

A. 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. For the mobile database system, safety strategy could better manage protect and distribute the sensitive and important information of mobile database..

1. Perfecting the Authentication Mechanism

In order to prevent illegal terminal access deceptively and background data may be damaged, it need for identity authentication, when mobile clients and service database operating synchronous in the mobile database system. When it needs to connect or disconnect mobile clients, the mobile database needs to carry on identity verification itself, since the users input their user name and password, so can query, modify the
local caching after verification in mobile clients. But the mobile customer is required to verify identity in the database server when the mobile client and the database server communicating. The following measures could be adopted.

• WPKI (wireless public-key system) can effectively solve the problem of identity authentication database. WPKI grant issue certificates for users and service providers, users in the transaction process using the certificate to ensure the confidentiality of the process of data transmission, integrity, and no repudiation, and complete the authentication of communication.

• Using triple encryption authentication methods of the class of Kerberos verify authentication. Firstly, in order to verify whether the test data is sent by the authentication server, mobile clients use the public-key of the authentication servers to verify the encryption data on the server and decrypt, secondly, the decrypted data is decrypted to obtain the relevant data again, then randomly generated a session keys, then server database once again receive the data before using the private key to decrypt the data, Session key and then use conventional methods of encryption and decryption to decrypt that data is issued by the authentication server, finally mobile database send a confirmation message, to verify the confirmation message is issued by the server-side database, the first opportunity to use mobile clients, the second opportunity to confirm the private key of the server-side database is encrypted. When the mobile clients receive confirmation message, they can use the session key encryption to communicate the server-side database with

• Establish strict user identification system. The operating system user authentication mechanism and the mobile database system are implemented together with the identity authentication mechanism to form dual protection. Such a dual user authentication mechanism to some extent to strengthen the confidentiality of the database system. This ensures the confidentiality of data, in particular, to ensure confidentiality of sensitive data on access control.

• Provide mobile users with identity protection. Prevent the information of mobile database users to leak or track. With the combination of CDMAlx and VPDN, firstly CDMA using spread spectrum technology, the strong anti-interference ability and confidentiality is also very good. Another CDMA system using fast switching power control technology, CDMA eavesdropping equipment is difficult to decipher the code, making it difficult to access mobile data, and ensure data security.

Secondly, the server of CDMAl x network side bind login user name with identification number. It is validated before access CDMA networks. Lastly the server authentication certificate of user network side can be achieved on the relevant members of the identity authentication to correctly identify the member user name and password

B. Further Strengthen Storage Access Control

The access control needs protection data determine to grant and implement authority. To flexible control database security, database management system should provide dynamic security mechanisms, such as dynamic authorization. Data processing is conducted by mobile devices, therefore database system allows database administrator and specific access users selectively dynamically grant access to other users. But if users need to access the resources of mobile database, it must register to the user assign a password and grant their visit corresponding system resources rights. Unauthorized arbitrary users could not use the database resource. To enhance database security, it can always change user password.

C. Strengthen the Encryption of Data

Access control alone is not enough to enhance privacy, and the mobile database system stored data is very important, Therefore it need to be encrypted to prevent leakage. Firstly it needs to set a password encryption, according to the functional modules of different database to set different levels of passwords, and password should be encrypted. Password security can use the method of zero, so that the genuine authorized user of the password cannot be pretending to copy or damage. Secondly, it can use different encryption methods, such as the use of elliptic curve cryptography (ECC). It is based on the intractability of the definition of point group in the elliptic curve discrete logarithm problem, thus increasing the database data security, and now there are no effective methods of attack break. In addition it can also use triple encryption authentication of the class of Kerberos or other encryption methods.

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 operation record of database could be recorded in the audit log automatically when the database is running, thus to monitor the operation to database of each user. The attack detection system detects the internal or external attacker attempts based on audit data, to reappear the events caused the system to the status quo, to analyze the system security vulnerabilities, track down the responsible person, so as to effectively guarantee the safety of mobile database.

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

The data of mobile database are usually very important, therefore 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

The safety of mobile database has great relevance with the use of mobile technology, so the relevant mobile technologies in the implementation should be taken safety measures. Such as 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.

B.SECURITY RELATED TECHNIQUES

1. Secure network connection

The mobile database and the central database have to be synchronized at specific times. The synchronization is implemented in the system software of the mobile database and is performed over the http protocol. Using http has the significant advantage of using a widely available protocol and possibly the disadvantage that its performance may be lower than a proprietary protocol for the database synchronization operation. We have selected the secure http protocol (https) to perform the necessary synchronization operations between the mobile and the central database. More precisely we use https with server and client authentication. This choice assures:

· Confidentiality of the data that is transferred.

· Authentication of the server computer.
· Authentication of the client computer.

Even though client authentication worked on the mobile platform we did not manage to apply it within the synchronization process of the mobile database. We believe that this is due to a shortage of the current system software and that will be overcome in the forthcoming versions.

2. Encrypted local database

The local database on the mobile device is encrypted and each time the user opens the mobile database, he has to enter his password. In case the mobile device is stolen or violated by an intruder, the data that is stored on the local database is not readable. The encryption algorithm is part of SQL Server Mobile
Edition and unfortunately we were not able to find documentation for the specific algorithm. We assume that the vendor does not simply rely on obscurity and that the encryption is based on one of the established symmetric key encryption algorithms. If the build-in encryption algorithm of the mobile database is considered insufficient, it is of course possible to implement this feature within the client application.

3. User authentication at the database server

The synchronization of the small-footprint database that is installed on the mobile device with the central database is performed with database replication technology. For this purpose, there is an appropriate publication at the database server. A publication is the meta-data package of information about which data is replicated. The mobile database uses the publication of the database server for the synchronization operation. In order to connect to the publication an appropriate user account on the database server has to be used. This means that the application user has to be authenticated at the database server.

4. Authentication at the web server

As already noted, the communication between the mobile database and the central database is performed over https. At the server side the communication link is handled by a web server. Hence, it is possible to take advantage of standard web server authentication and require the user to authenticate at the web interface level. This requirement is very important since it provides protection for the mobile database agent that is executed at the server side within the web server. Without web server authentication every network user would be able to contact the server-side agent by simply using the appropriate URL.

5. Server-side mobile agent account

Both endpoints of the communication link are handled by mobile database agents. During a synchronization process, the agent operations on the server-side can either be executed by the default agent account of the server's operating system or in the context of a dedicated account of the server's operating system. We use a dedicated operating system account for the execution of the agent service.
The account has been granted the minimum permissions that are necessary for its role. This decision satisfies the common security rule of granting minimum sufficient permissions.

6. Separate user accounts for the authoring and the read-only application

In case a user has to use the application both as an author of announcements and as a reader of all announcements we can either assign two accounts to the user, an authoring account and a read-only account, or grant both functionalities to a unique user account.
Even though the security of the application would not be lowered by using a unique account, we preferred to use two separate, dedicated accounts. This approach reflects in a more natural way the structure of the application.

7. Application provided security

For authoring operations, each user has access only to his own data. A set of database triggers implemented in the database server, check that the data manipulation operations of the user are valid. This check prevents all users from accidental or malicious modifications of data for which they have no authorization. More precisely, an author

– can create new announcements that are signed with his name,
– can delete or update announcements that are signed with his name, and
– has no access to announcements created/signed by other users.

The above functionality resembles in a loose sense the virtual private database technology (VPD) of Oracle [9].

8. The read-only client

The read-only part of the MDA is implemented as a separate client application. The read-only client provides access for viewing all announcements. We apply certain techniques to assure the security of the central database:

– The publisher of the database server that is used for the synchronization of the read-only application is defined to be read-only. Consequently it is not possible to apply any modification to the central database from the read-only application.

– Read-only clients have no access to the main table of the central database. Instead the read-only clients read the announcements from a replicated instance of the main table. A set of database triggers implemented in the database server keeps the replicated table always updated. In case an accidental or malicious modification of the data in the replicated table would occur, it would have no effect on the main table of the application.

9. Communication between the servers

The announcements are also available over http as a web page. A dynamic web page with aspx code gives a list of the announcements. The web server must have access to the database in order to read the data. For this reason we have to deal with a common security issue in database-driven web sites: Choosing the appropriate database account that the web server is using to access the database. We created a specific account in the database that has only one permission: To perform a select on the replicated announcements table. This decision too, applies the principle of granting the minimum sufficient permissions.

10. Client-side data encryption

We also tested a common but very important feature, that of encrypting the user data in the database. Even though this feature is not directly relevant to the announcements application, we consider it very important for secure mobile database applications and more generally for secure database applications. The user gives a password to the client application and all his critical data is encrypted at the client-side before it is permanently stored in the database. This encryption guarantees the confidentiality of the data against any database user including the local database administrators.

The approach is very simple:

The client application applies a symmetric key encryption algorithm, for example AES, and stores the encrypted data into the database. When the user reads the data, he provides his password and the data is decrypted. We verified this approach and it works transparently as soon as the user has given his password.

A shortage of the current mobile platform was that some library functions, like for example the function ”PasswordDeriveBytes”, were not provided by .NET

Compact Framework v2.0.We overcame this problem by providing a hand-coded implementation of the required function that was absent.

C. Major issues in multilevel security on Distributed Security Manager

Authentication
Data confidentiality
Identification and
Enforcing appropriate access controls.

1) Authentication

User authentication is the primary line of defence for mobile and handheld devices such as Personal Digital Assistants (PDAs). Authentication determines and verifies the identity of a user in the system, i.e., providing an answer to the question: “Who is the user?” Traditional authentication mechanisms rely on maintaining a centralized database of user identities, making it difficult to authenticate users in a different administrative domain as depicted. This mechanism for providing security in mobile device is a difficulty for every system providing safe access to precious, private information, or personalized services. Issue here is the authentication mechanism should be distributed, and the various components of the authenticator need to communicate with each other to authenticate a user. In centralized environment, the authenticator needs to have information about all of the users of the system.

There are three basic authentication means by which an individual may authenticate his identity.

a) Something an individual data (e.g., a password,Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).

b) Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).

c) Something an individual IS (Intermediate System) (e.g., personal characteristics or "biometrics" such as a fingerprint or voice pattern), this technique works on the Fingerprint basis whereby the phone can be accessed when it identifies the Fingerprint of the user(s). Mobile device user need only authenticate him to the first device he logs into and that device passes the authentication data to each of the other devices then the user can to access. This scheme requires that all of the devices on the network are capable of reliably handling this authentication data. Standardization efforts such as Open System Environment(OSE), Portable Operating

System Interface (POSIX) and Government Open Systems Interconnection Profile (GOSIP) can contribute to this goal of transparent authentication across networks.

By notation to three basic authentication means that we describe, PIN based authentication is a method for verifying the identity of actual device users, but this method have considerable drawbacks, because pick PIN or passwords can be easily guessed. For prevent guess a password, user have to defines a complex password, then it is often hard to remember. To address this problem in handheld devices, have developed comparatively more secure, affordable and memorable authentication schemes based on graphical assistance or Biometric authentication, such as fingerprints, voice recognition, iris scans, and facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable.

2) Data confidentiality

Typically, the increasing connection of travelling users to corporate databases to make personal data available to mobile users introduce new threats on data privacy and confidentiality. Nowadays, one solution is considered that called C-SDA (Chip- Secured Data Access), which allows querying encrypted data while controlling personal privileges. C-SDA is a client-based security component acting as an incorruptible mediator between a client (potentially mobile) and an encrypted database. This component is embedded into a smart card to prevent any tampering to occur on the client side. It is better to embed the user's confidential data into her own mobile device (e.g., a PDA). Apart from their limitation in terms of storage capacity, even these devices cannot be fully trusted because they can be stolen, lost or destroyed (thus a copy of the data they host has to be maintained in the network to guarantee data resiliency) Another way to provide confidentiality is through encryption, either using the public key of the receiving principal or using a combined symmetric key and public key method. For instance, the agent can be encrypted using a symmetric key and the symmetric key protected using the public key of the receiving principal. Encryption often used to protect data on insecure networks or storage devices.

3) Identification

The process of verifying a user's identity is typically referred to as user identification and authentication. Passwords are the common method used for authenticating computer users, but information as name (e.g. First or last) or a Passwords, email address provides no assurance of identity, in preventing unauthorized access to computer resources when used as the sole means of authentication, so some users are beginning to use biometrics as methods of user identification. If we want use from passwords as security means so have to management use of passwords by Periodic changing of passwords that it depends on the sensitivity of the data, or use of deliberately misspelling words, combining two or more words together, or including numbers and punctuation in a password, so that prevent the guess of passwords. The identity must be unique so that the system can distinguish among different users. The identity should also be non-forgeable so that one person cannot impersonate another. An important distinction between identification and authentication is that identities are public whereas authentication information is kept secret and thus becomes the means by which an individual proves that he actually is who he claims to be. In addition, identification and authentication provides the basis for future access control.

4) Access control

Access control protects data integrity by limiting who can alter data. The access control rules enforced in a distributed environment may be distributed, centralized or replicated. If the rules are centralized, then the central server needs to check all accesses to the database. If the rules are distributed, then appropriate rules need to be located and enforced for a particular access. Often the rules associated with a particular database may also be stored at the same site. If the rules are replicated, then each node can carry out the access control checks for the data that it manages Relational database systems implement access control in the SQL language, using the GRANT and REVOKE commands. The GRANT command is used to give privileges to users.

IV. TECHNIQUES AND TECHNOLOGY

Solution for Securing of Mobile Network

For mobile operators, the first step in defeating attacks on their networks is to recognize their newfound role as an ISP. This means implementing a layered defense for their network that:

_ Changes security policies and practices to better reflect the new threats

_ Concentrates, whenever possible, wireless data services into a smaller number of data centers. Many mobile operators in Europe have already taken these types of steps to protect their core networks

_ Protects end users by implementing technology on their devices and in the network – e.g., anti-virus, firewalls, content scanning – that provides file-level security

_ Deploys security products such as firewalls, virtual private networks (VPNs) and intrusion detection and prevention (IDP) systems at appropriate points in the network, which

_ provides packet level, session level and application level protection securing the Mobile Network

V. CONCLUSION

This paper with the continuous promotion of mobile computing technology and use of mobile database technology, the data security becomes an issue. The security policy of mobile database described in this article can guarantee the safety in practical application, but security strategy also requires a specific treatment based on the actual issues. So it's important to continue to explore the security issues of database system in the mobile environment The emerging trend is to make all service providing disciplines, such as web, E-commerce, workflow systems, etc., fully mobile and secure so that any service can be provided from any place. Customer can surf the information space from any location at any time and do their shopping, make flight reservation, open bank account, attend lectures, and so on.

- Trust assumptions are different in the Internet
- Enhanced levels of security services may be necessary
- Public-key cryptography can provide effective solutions
- Try not to preclude future provision of improved security services

Finally, an important issue is the lack of appropriate documentation for certain encryption algorithms that are used within the system software of mobile platforms.

REFERENCES

1. Ramez Elmasri and Shamkant B. Navathe. Fundamentals of Database Systems, 4th Edition. Addison-Wesley, 2004.
2. Benjamin Halpert. Mobile device security. In InfoSecCD ’04: Proceedings of the 1st annual conference on Information security curriculum development, pages 99–101, New York, NY, USA, 2004. ACM Press.
3. Sushil Jajodia. Database security and privacy. ACM Comput. Surv., 28(1):129– 131, 1996.
4. Sumit Jeloka. Oracle Database Security Guide. Oracle Corp., Redwood City, CA, USA, February 2005. B14266-01.
5. Abraham Silberschatz, Henry F. Korth, and S. Sudarshan. Database System Con-cepts, 5th Edition. McGraw-Hill Book Company, 2005. M. N. DOJA, NAVEEN KUMAR, user authentication schemes for mobile and handheld devices, Jamia Millia Islamia - New Delhi,2007]
6. L. Bouganim, P. Pucheral, "Chip-Secured Data Access: Confidential Data on Untrusted Servers", Int. EPFL, U. Grenoble, INRIA-Nancy, INT-Evry, U.Montpellier, U.Paris, U.Versalles, Mobile Databases: a Selection of Open Issues and Research Directions, SIGMOD Record, Vol. 33, No. 2, June 2004
7. Identification and authentication, NIST Computer Security Handbook lker Köse, Distributed Database Security, Data and Network Security - Spring 2002
8. K. Johnson, The Design of Secure Mobile Databases: An Evaluation of Alternative Secure Access Models. A Master's paper for the M.S. in I.S. degree. August, 2002. 110 pages. Advisor: Stephanie W. Haas.
9. S. P. Coy, Security Implications of the Choice of Distributed Database Management System Model: Relational vs. Object-Oriented, 1997

