Secure Access Schemes in Mobile Database Systems

MIN-SHIANG HWANG
Department of Information Management,Chaoyang University of Technology,
Wufeng, Taichung, Taiwan 413, ROC.
E-mail: mshwang@mail.cyut.edu.tw
http://www.cyut.edu.tw/~mshwang/

CHII-HWA LEE
Universal Exchange Inc.
NanKang, Taipei, Taiwan, ROC.

Abstract. Mobile computing is a newly emerging computing paradigm. Whether using the term mobile database system or some other form, the database concept is essential to the mobile computing environment. This work employs a more thorough yet general means of defining the mobile database system, along with several application scenarios. Possible secure access schemes are also presented for databases in a mobile computing environment. The tradeoffs of these schemes are also analyzed. Moreover, the feasibility of applying some possible secure access methods is explored, along with the potential difficulties and unresolved issues. Finally, concluding remarks and recommendations for future works are made.

Keywords: encryption; mobile computing; mobile database system; security..

1 INTRODUCTION

A mobile computing environment, consisting of mobile communications and distributed computing, heavily influences conventional information systems or database systems. In mobile database systems, mobile hosts have severe resource constraints in terms of limited battery life and limited non-volatile storage size. Both site failure and frequent voluntary shut downs of the mobile host produce more problems for mobile database systems. Under the circumstances of power constraints and frequent mobile host disconnection, the burden of computation and communication load cannot be distributed equally among static hosts and mobile hosts.

The mobile database concept has been proposed in the literatures. We describe briefly the literature as follows. Imielinski and Badrinath offered some database concepts regarding information services in a mobile computing environment [21]. The main concept was that mobile users would be database producers as well as consumers. Such a database may be stored both in mobile as well as at static hosts and updated and queried over wireless connections. Dunham and Helal presented a classification, including mobile database management systems; for distributed database management systems based on autonomy, distribution, and heterogeneity system characteristics [8]. Elmagarmid, et al., proposed architecture alternatives for information services in wireless client/server computing [10]. These researches about data replication [11,14] aimed to optimize the communication cost between a mobile computer and a stationary computer that stored the online database. Pitoura and Bhargava provided a framework for agent-based access to heterogeneous mobile databases, explored the implications of such a model, and identified the aspects in which it differs from traditional database models [26,27].

Many researchers have proposed various protocols or strategies to deal with query and transaction processing issues [1,11,14,20,22,30,32]. However, security and privacy related issues involving access to mobile databases have largely been neglected. As security and privacy remain sensitive issues in mobile computing, many wireless communication systems have developed their own security schemes. Moreover, many investigators have examined the authentication of mobile users, the data confidentiality of communications and location privacy of the users [4,15,16,19,23,31]. However, those studies have not addressed a critical security aspect of the mobile computing environment: secure *access schemes* and control methods for mobile database systems.

The rest of this paper is organized as follows. More detailed descriptions of the characteristics of a mobile database system are given, along with several application scenarios. Possible secure access schemes are presented for databases in a mobile computing environment. The

tradeoffs between these schemes are also analyzed. Moreover, the feasibility of applying some possible secure access methods is explored, along with the potential difficulties and unresolved issues. Finally, concluding remarks and recommendations for future works are made.

2. MOBILE DATABASE SYSTEMS

2.1 MOBILE DATABASE SYSTEM ARCHITECTURE

Figure 1 depicts the architecture of a mobile database system. The architecture consists of mobile and stationary components. The stationary component is the Fixed Hosts (FH), which are connected together via a fixed high-speed network. Some of the FHs, Mobile Support Stations (MSS), are augmented with a wireless interface to communicate with Mobile Hosts (MH) located within a radio coverage cell. The mobile component is the Mobile Units (MU), or MHs, which are connected to the fixed network and communicates with the FHs or other MUs via a wireless channel. Each FH or MH can have a database system which can locally or globally provide services not only to mobile users but also to the fixed users who are located on the fixed network. MSS play a critical role in transmitting the queries and transactions from mobile users to other fixed or mobile hosts. A mobile user may be the "home" user who initially registers in this MSS. Herein, we denote this MSS as H-MSS. A user may be a "visiting" user who is currently visiting in the coverage of this MSS. We denote this MSS as V-MSS. Therefore, the MSS functions in the role of either a "delegate" of the mobile users when the MSS processes some operations for the users or a "coordinator" of transactions for other hosts.

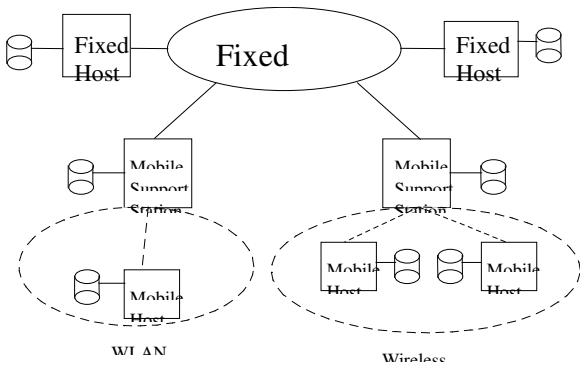

Figure 1. Mobile Database System Architecture

2.2 CHARACTERISTICS OF MOBILE DATABASE SYSTEMS

A mobile database system has the following features:

- A database can be *stationary* or *mobile*. Both mobile and fixed users can access the database, regardless of location.
- The queries and transactions provided by mobile users could be processed during users' movement [10]. The query processing and transaction management is transparent to the mobile users.
- Disconnectivity or failure of a mobile host complicates the access when the mobile host provides a data service for a specific application. Therefore, disconnectivity management and data consistency are of primary concern in accessing mobile database systems.
- The queries and data transmissions via wireless channels between users and database systems should be minimized due to the bandwidth limitations of wireless channels and power constraints of mobile hosts.
- According to the types of information services provided by the database systems, mobile users can dynamically change access to different databases while moving to new service areas.
- *Heterogeneity* is the consequence of an expected increase in the scale of distributed systems with the introduction of mobile hosts. Dunham and Helal [8] viewed a mobile computing database environment both as an extension and a dynamic type of distributed system where links between nodes in the network dynamically change. Thus, a mobile computing database environment can be appropriately viewed as a *Mobile Heterogeneous Multidatabase System*.

Based on the above characteristics, we deem *mobile database systems* as classes of multidatabase systems in which constituent databases may reside on mobile hosts and/or stationary hosts in a mobile computing environment.

2.3 APPLICATION SCENARIOS

The potential applications of mobile database systems are described as follows:

(1) Exploration Operations and Sensor Value Reading Scenarios:
Some exploration operations could use mobile hosts to accumulate data in rural areas, jungles or desert areas. The fact that the data volume for this type of accumulation is usually large would make it feasible to locally analyze raw data and then store the results in the mobile host. Thereafter, other related users, possibly in the headquarters of a company on fixed hosts or on other mobile hosts, can query the information via the fixed network and wireless channels.

(2) Military Application Scenarios:
Mobile communication plays a critical role in transmitting data and voice in military applications. A typical example of using mobile database systems is the Aircraft Carrier and the fleet. An Aircraft Carrier has a local database system to provide services to local users, to the users in the fleet, and even to users

in the headquarters on the land for some specific applications. The database of an Aircraft Carrier is mobile when it provides services to those mobile or fixed users. On the other hand, users on the ships of the fleet can access not only the databases on the mobile hosts of an Aircraft-Carrier, but also the databases on the fixed hosts on land through wireless links.

3. SECURE ACCESS SCHEMES

Most security concerns focus on mobile communications [12,24]. Accessing mobile databases has received only limited attention. The primary issues involving conventional database protection requirements include protection from improper access and inference, user authentication, database integrity, and protection of sensitive data [5]. Since the mobile databases may be on mobile and/or stationary computers, the *mobility* and *disconnectivity* complicate the protection mechanisms for accessing databases. Many access control methods are available in the existing distributed database systems [3]. However, those methods do not completely cover the special concerns involving the bandwidth and energy management of mobile hosts.

3.1 THE MODEL

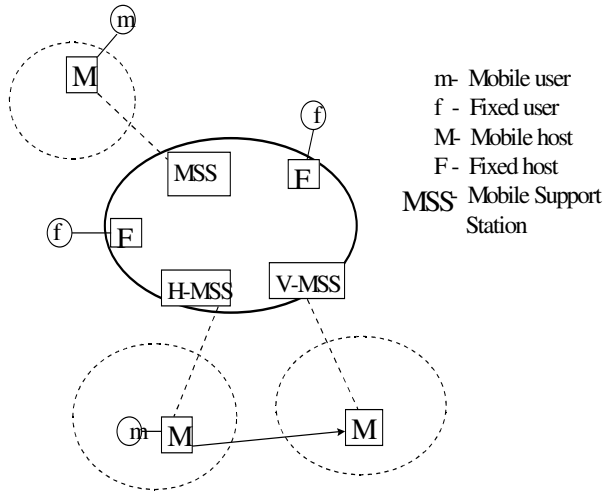

Figure 2. Access Model

Figure 2 depicts the access model for mobile database systems. H-MSS and V-MSS denote the home and visiting domain Mobile Support Stations, respectively. H-MSS is not only responsible for the communications for a mobile user (denoted as M) but also provides M authentication information to another MSSs when M moves into new cells. When M moves to a new cell, the V-MSS take charge of the communications for M. The mobile host, M, maintains a database system that can be accessed by all kinds of users. The mobile hosts may have the following states:

(1) Active mode - Registers in a MSS and remains active.
(2) Sleep mode - Registers in a MSS and temporarily remains in a sleep mode for sake of power saving.
(3) Inactive mode - Turns power off, or disconnects with its current MSS, without de-registering or leaves the coverage of an MSS.

Figure 3 depicts the states and transitions of mobile host. When a mobile host registers in a MSS and communicates with this MSS, the mobile host is in an active mode. In the active mode, the mobile host can request services from the networks or provide on-line data access to the users. If the mobile host is disconnected, which is due to failure or voluntary shut downs, the current state (active) of the mobile host will be transited into inactive. If the users no longer access the mobile host for a while, the current state (active) of the mobile host will be transited into sleep for the sake of saving power. When a mobile host registers in a MSS and temporarily stops providing service for the sake of saving power, the mobile host is in the sleep mode. In the sleep mode, the mobile host temporarily remains in the energy-saving status and does nothing active. If a mobile user wants to access the mobile host, the MSS sends a message to trigger the mobile host into the active mode. If the mobile host is disconnected, which is due to failure or voluntary shut downs, the current state (sleep) of the mobile host will be transited into inactive. When the mobile host turns the power off, or disconnects with its current MSS, without de-registering or leaves the coverage of a MSS, the mobile host is in an inactive mode. From the inactive mode to the active mode, the mobile host must re-register with a MSS again.

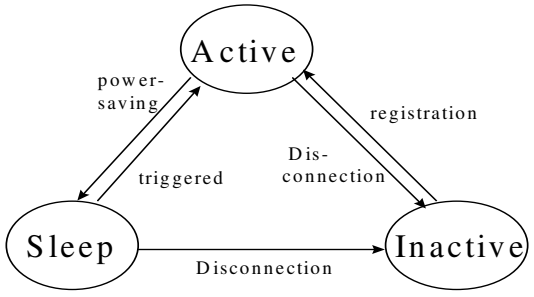

Figure 3. Mobile host' states and transitions.

We denote four access types of users in our model for next two subsections.
Access Type A: Fixed users (f) access fixed databases (F);
Access Type B: Fixed users (f) access mobile databases (M);
Access Type C: Mobile users (m) access fixed databases (F);

Access Type D: Mobile users (m) access mobile databases (M).

We propose two secure access schemes: *Direct Access* and *Indirect Access*, in the next two subsections.

3.2 DIRECT ACCESS SCHEME

In the Direct Access (DA) scheme, the hosts autonomously maintain a primary copy of the data. The main functions of MSSs herein are to manage the locations of mobile hosts, as well as transmit the queries and results for users and database systems. When the user sends a query, the authority check is eventually processed by the accessed database system regardless of the access type. The DA operations for different access types are described as follows:

Type A - The access is the same as that for distributed database systems. The Local Database Management System (DBMS) knows the address of the target machine of the accessed database and directly requests data. The target DBMS manages user access.

Type B- The local DBMS must initially identify which MSS is the nearest to the mobile host, pass the queries to this MSS, then waits for a response from the MSS. The MSS transmits the queries and receives the response to/from the mobile host. All database access is manipulated by the mobile database system.

Type C- The local MSS of the mobile user knows the address of the target machine of the accessed database in the network. It manages the queries and transactions for the mobile users. This access resembles distributed database systems.

Type D- Three connections are available for passing the queries: mobile user host to its MSS, local MSS to remote MSS, and remote MSS to a remote mobile host. The local MSS must find the remote MSS and then transmit the queries to it, whereas the remote MSS must connect to the mobile host.

For types B & D, when the remote MSS receives the queries and the target machine is in the active mode, the connections between users and the remote mobile host are established. The user can then directly have on-line access to the database. If the target machine is in the sleep mode, the MSS triggers the mobile host first. The connection and direct access can then be set. If the target machine is in the inactive mode, connection failures could occur.

3.3 INDIRECT ACCESS SCHEME

.

For bandwidth, energy management and disconnectivity of mobile hosts, an Indirect Access (IA) scheme, or *Database Replication Scheme,* can be considered for application to access types B and D. In this scheme, a whole portion or fragments of the mobile database are duplicated to the MSS in the registration phase. The MSS acts, thereafter, on behalf of the mobile database to *provide*, not to *manage*, the data to mobile users regardless if the mobile database is in the active, sleep, or inactive mode. Theoretically, the accessed database is still responsible for user access; however, the check operations can be executed in the MSS.

When a user sends the queries to network, the network must initially locate the V-MSS, which the mobile database is currently located under its coverage. Since V-MSS has the replicas of the mobile database, on-line transactions can be immediately processed on the network, not necessarily on the mobile hosts. Under this circumstance, access type B and D can be treated as type A and type C, respectively.

A mobile database system moving to a new cell must register in a new V-MSS. A mobile host belongs to, at most, one cell and this can be achieved by an appropriate handover mechanism. The old data copy in an old MSS can be either maintained on a disk (marked as *obsolete*) or completely deleted. Due to the characteristics of locality of a mobile host, maintaining obsolete data may offer some advantages while the mobile host could possibly move back. A critical issue about IA is *data consistency* between MSS and mobile database. Since different types of queries can access mobile database, read the data or write the data. Periodical data consistency operations are thus necessary.

For IA, detailed operations for different mobile host states are described as follows:

(1) Mobile host is active:
User queries are sent to the remote MSS and query processing is executed in the MSS. The MSS provides the data on behalf of the mobile database. Data consistency is maintained between the MSS and mobile database. If the mobile host is moving to a new cell during transaction processing, the location handover can be processed using appropriate mechanisms. However, the data replications, which reside in the current MSS for the mobile database, require some deliberative designs to cope with the mobile database. In particular, MSS replica handover timing is essential in managing mobile database movements.

(2) Mobile host is in the sleep mode:

When users send queries to a remote MSS, the MSS processes the queries. The MSS triggers the mobile host to be active if the mobile host is in the sleep mode. Periodic data consistency operations can then be executed.

(3) Mobile host is in the inactive mode:
The remote MSS processes the queries sent by users. The MSS logs the transaction content, i.e. read or write. If the mobile host is disconnected during the transaction processing, the transaction for updating data is marked as *incomplete* until a commitment is issued by a mobile database system. In this case, read only queries are lesser problems than read/write queries. The data consistency operation should be executed when the mobile host reconnects to the MSS. Dirty records are then written to the mobile database. However, it is possible that a transaction cannot be completed due to a data conflict. Then, the *incomplete* transaction becomes *aborted*. Therefore, a *conflict resolution* mechanism for IA must be designed as well.

3.4 COMPARISONS OF DA WITH IA

DA offers advantages in that the access mechanism is controlled by the accessed database system and encryption overhead for its data can be averted. The MSS only passes the data, but does not own the data nor have knowledge of the data. The problems, however, include (a) a large bandwidth is necessary for the transactions between the MSS and mobile databases, (b) the power consumption of mobile database hosts is increased, and (c) the accessibility of the mobile database is decreased. Therefore, this scheme is inappropriate for access types B and D, but more suitable for mobile users requesting services from fixed hosts, i.e., access types A and C.

IA offers advantages that remedy the DA weaknesses. However, the limitations of this scheme are that (a) overhead is necessary to periodically maintain data consistency between the replicas and local databases and (b) some secure mechanisms are required to protect the data stored in the V-MSS. While a mobile host moves to a neighboring area, the V-MSS stores the entirety or fragments of the replicas of its database. The major concern here is that without authorization, the V-MSS must not be able to read, write or modify the databases. The V-MSS only provides storage for the data and processes transactions for the queries, but does not have any knowledge about the data.

4.SECURE ACCESS SCHEME IMPLEMENTATION CONSIDERATIONS

Despite the access mechanism characteristics in general distributed database systems, from an information security perspective, mobile database systems should have the following additional requirements.

(1) Without authorization, the MSS, which transmits the data or even maintains the replicas of other host databases, must not read, write or modify the data. Regardless if the MSS is the delegate of the users or the coordinator of the hosts, the MSS can not have knowledge of the data if the MSS does not have authorization.

(2) The accessibility to the mobile databases should be maintained at the maximum level. As is generally known, high availability is a prerequisite in information services. The disconnectivity management can reduce or interrupt users' on-line access to the mobile database.

(3) The communication cost or energy consumption should be minimum, or at least reasonable, for the mobile hosts. Bandwidth limitations and power constraints are the critical concerns in designing a mobile computing system. Also, reducing transmissions or maintaining reasonable transmissions via wireless channels is always a primary object.

To implement secure access schemes for IA, two promising methods are introduced, based on the above requirements: the *Database Encryption method*, and the *Database Compression method*.

4.1 DATABASE ENCRYPTION METHOD

From the perspective of DBMS security, controlling the disclosure of confidential data in a distributed database system is extremely difficult. Also, verifying the authentic origin of a data item is also difficult if raw data exists in a readable form inside the database. The general solution is to use encryption to enforce database security. Database security based on encryption includes database encryption systems with a single key [13] and subkeys [7,17,18]. The first method requires a trusted centralized access scheme from which to control all access to the databases. All encryption and decryption are executed by the trusted access scheme with a privacy key. In the second method, however, the users execute decryption with their own deciphering subkeys.

For encryption/decryption databases with subkeys, enciphering subkeys (or named public key) is used to encryption tuples of all records [17,18]. And deciphering subkeys (named privacy key) is used to decrypt and to obtain the confidential information from the mobile databases. In this scenario, mobile users must initially achieve the authorized subkeys from mobile databases, then they can query the database with their own subkeys. Mean-

while, the MSS only maintains the encrypted replicas of a mobile database. The MSS, without the legal subkeys authorized by the database system, cannot access the data. This measure ensures that the MSS only plays an agent role in providing data and can not eavesdrop on the data.

To fulfill the requirements of a mobile database environment, this method offers the following advantages. (1) No mobile user can directly read, write, destroy, or modify data if he does not have the legal subkeys. (2) The security mechanism does not significantly degrade the performance of the basic database operations [7]. (3) The MSS plays an agent role in which the confidentiality of the database is ensured. (4) All users can always access the MSS. The accessibility of the database system is not reduced whether the mobile database system is in the active or disconnected mode. (5) The encrypted data replica is reduced in size. The replica transmissions and data consistency control do not increase between the MSS and the mobile database system.

4.2 DATABASE COMPRESSION METHOD

Several compression techniques have been proposed for compressing statistical databases [6,9,25]. These techniques include run-length encoding, order-preserving compression index encoding methods, Huffman's encoding method and its variations, and tuple differential coding. Data compression techniques can have a positive cost effect on the storage and transfer of data. Based on Bassiouni's and Severance's descriptions [2,29], we summarize some benefits of database compression, particularly for a mobile computing environment.

(1) Reducing storage requirements in both the mobile host and mobile support station.
The most obvious advantage of database compression is reducing the storage spaces. The mobile host has the characteristics of smaller size and smaller capacity. Reducing storage requirements is obviously an attractive issue in memory management. Since the MSS acts the transient point or the repository for much information in mobile computing, storage management is still an important issue.

(2) Increasing the data transfer rate:
Since compressed data are encoded using a smaller number of bytes, transfer of compressed information from one place to another requires less time. Most important is the data compression application in reducing the cost of data communications. This application is becoming increasingly important due to the fact that great cost savings can be achieved by compressing voluminous amounts of data before it is transmitted over wireless communication links with limited bandwidth.

The IA access scenario using the database compression method is as follows: The mobile host initially compresses the database and transmits the compressed replica to the local MSS. When a user requests data, the MSS only *partially* decompresses the replica, according to user's queries for specific tuples, fields or statistical results. The MSS then encrypts and sends the query results using the user's enciphering subkeys. This method can decrease the number of transmissions between the MSS and mobile database. The MSS during this process cannot read the compressed database.

In order to accommodate the database compression techniques to secure access in mobile databases, database compression with a partial decompression technique should exhibit the following features [25]:

(1) Tuple access should not require massive compression and decompression. One would not use a compression technique that decompresses and recompresses the entire database every time a tuple is accessed. Thus the scope of compression should be reduced.

(2) The system should provide localized access to compressed tuples. One must be able to build access mechanisms in a compressed database.

(3) Compression and decompression should be fast enough so as not to offset its advantages, i.e., a database compression technique should not be so complex as to offset its space and bandwidth reduction advantages.

(4) The tuple structure of a relationship should be preserved. One would like to be able to access each tuple individually.

Bassiouni [2] and Roth & Van Horn [28] mentioned the fact that the literature on data compression is rich and growing, but little has been done to compare the different techniques or identify the best compression scheme for a given environment. A benefit of comparing methods is the possible integration of a number of appropriate compression techniques applied to subsets of the database, instead of just one technique, which works marginally on the entire database. Another benefit may be the combination of two or more methods in a single algorithm.

5. FUTURE WORKS AND CONCLUSION

This work employs a more thorough yet general means of defining a mobile database system. Mobile database services have a large market potential for both commercial and military applications. However, transaction management, query processing, and access control methods for mobile databases must be revisited and redesigned. Two database access schemes were also presented. Although we have explored the possible secure access meth-

ods for a mobile database system, some problems must be resolved before introducing the methods originated for a distributed system or a traditional database system. Future works should include both the *timing* and handover *mechanisms* among MSSs for mobile database systems and *conflict resolution* for data consistency in an IA scheme, modifying the encrypted database with the subkey method and designing algorithms for the compression and partial decompression methods.

ACKNOWLEDGEMENTS

The authors wish to thank many anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-025.

REFERENCES

[1] R. Alonso and H. F. Korth, "Database System Issues in Nomadic Computing," Proc. of the ACM SIGMOD, 1993, pp. 388-392.

[2] M. A. Bassiouni, "Data Compression in Scientific and Statistical Databases," IEEE Trans. On Software Engineering, Vol. 11, No. 10, Oct. 1985, pp.1047-1058.

[3] D. Bell and J. Grimson, *Distributed Database System*, Reading, Mass., Addison-Wesley, 1992.

[4] M. J. Beller, L. F. Chang and Y. Yacobi, "Privacy and Authentication on a Portable Communications System", IEEE J. on Select. Areas in Commun., Vol. 11, No.6, Aug. 1993, pp.821-829.

[5] S. Castano, m. G. Fugini, G. Martella, and P. Samarati, *Database Security*, Addison-Wesley Publishing Company, New York, 1995.

[6] G. V. Cormack, "Data Compression on a Database System," Communication of the ADM, Vol. 28, No. 12, Dec. 1985, pp. 1336-1342.

[7] G. I. Davida, D. L. Wells, and J. B. Kam, "A Database Encryption System With Subkeys," ACM Transactions on Database Systems, Vol. 6, No. 2, 1981, pp.312-328.

[8] M. H. Dunham and A.(Sumi) Helal, "Mobile Computing and Databases: Anything New?," SIGMOD Record, Vol. 24, No. 4, December 1995, pp.5-9.

[9] S. J. Eggers, F. Olken, and A. Shoshani, "A Compression Technique for Large Statistical Databases," Proc. Seventh Int'l Conf. Very Large Data Bases, 1981, pp. 424-434.

[10] A. Elmagarmid, J. Jing and T. Furukawa, "Wireless Client/Server Computing for Prsonal Information Services and Applications," SIGMOD Record, Vol. 24, No. 4, December 1995, pp. 16-21.

[11] M. Faiz and A. Zaslavsky, "Database Replica Management Strategies in Multidatabase Systems with Mobile Hosts," In Proceedings of 6th International Hong Kong Computer Society Database Workshop: Database Reengineering and Interoperability, Hong Kong, March 1995.

[12] L. Gong and N. Shacham, "Multicast Security and Its Extension to a Mobile Environment," Wireless Networks, Vol.1, 1995, pp.281-295.

[13] E. Gudes, "The Design of a Cryptography Based Secure File system," IEEE Trans. On Software Engineering, Vol. 6, No. 5, 1980, pp.411-420.

[14] Y. Huang, P. Sistla and O. Wolfson, "Data Replication for Mobile Computers," Proc. of the ACM SIGMOD, International Conference on Management of Data, Minneapolis, MN, May 1994, pp. 13-24.

[15] M. S. Hwang, "Dynamic Participation in a Secure Conference Scheme for Mobile Communications," IEEE Transactions on Vehicular Technology, Vol. 48, No. 5, 1999, pp. 1469-1474.

[16] M. S. Hwang and C. H. Lee, "Authenticated Key-Exchange in a Mobile Radio Network," European Transactions on Telecommunications, Vo1. 8, No.3, May 1997, pp.265-269.

[17] M. S. Hwang and W. P. Yang, "A Two-Phase Encryption Scheme for enhancing Database Security," Journal of Systems and Software, Vo1.31, No.12, December 1995, pp.257-265.

[18] M. S. Hwang and W. P. Yang, "Multilevel Database Security with Subkeys," Data & Knowledge Engineering, Vo1.22, 1997, pp.117-131.

[19] M. S. Hwang and W. P. Yang, "Conference Key Distribution Protocols for Digital Mobile Communication Systems," IEEE Journal on Selected Areas in Communications, Vo1.13, No.2, February 1995, pp.416-420.

[20] T. Imielinski and D. Barbara, "Sleepers and Workaholics: Caching Strategies in Mobile Environments," Proc. of the ACM SIGMOD, International Conference on Management of Data, Minneapolis, MN, May 1994, pp.1-12.

[21] T. Imielinski and B. R. Badrinath "Mobile Wireless Computing: Challenges in Data Management," Communications of the ACM, Vol.37, No.10, Oct. 1994, pp.19-28.

[22] N. Krishna Kumar and R. Jain, “Protocols for Maintaining Inventroy Database and User Profiles in Mobile Sales Applications,” In Proceedings of the Mobidata Workshop, October 1994.

[23] C. H. Lee, M. S. Hwang, and W. P. Yang, “Enhance Privacy and Authentication for the Global System of Mobile Communications”, Wireless Networks, Vol. 5, 1999, pp. 231-243.

[24] P. Lin and L. Lin, “Security in Enterprise Networking: A Quick Tour,” IEEE Communications Magazine, Jan. 1996, pp.56-61.

[25] W. K. Ng and C. V. Ravishankar, “Block-Oriented Compression Techniques for Large Statistical Databases,” IEEE Trans. On Knowledge and Data Engineering, Vol. 9, No. 2, March-April, 1997, pp.314-328

[26] E. Pitoura and B. Bhargava "Building Information Systems for Mobile Environments," Proc. of the 3rd Inter. Conf. on Information and Knowledge Management, Nov 1994, pp.371-378.

[27] E. Pitoura and B. Bhargava, "A Framework for Providing Consistent and Recoverable Agent-Based Access to Heterogeneous Mobile Databases," SIGMOD Record, Vol. 24, No. 3, Sep. 1995, pp. 44-49.

[28] M. A. Roth and S. J. Van Horn, “Database Compression,” SIGMOD RECORD, Vol. 22, No. 3, Sep. 1993, pp.31-39.

[29] D. G. Severance, “A Practitioner’s Guide to Database Compression: Tutorial,” Information Systems, Vol. 8, No. 1, 1983, pp.51-62.

[30] M. Tsukamoto, R. Kadobayashi and S. Nishio, “Strategies for Query Processing in Mobile Computing,” in *Mobile Computing*, edited by T. Imielinski and H. F. Korth, Kluwer Academic Publishers, Boston, 1996, pp.595-620.

[31] J. E. Wilkes, "Privacy and Authentication Needs of PCS," IEEE Personal Communication, Aug. 1995, pp.11-15.

[32] O. Wolfson, et al., “View Maintenance in Mobile Computing,” SIGMOD Record, Vol. 24, No. 4, December 1995, pp. 22-27.

BIOGRAPHY

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, 1999, 2000 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Chii-Hwa Lee received the BS degree from National Taiwan University, Taiwan, in 1976, the Master of Computer Science from Texas A&M University, USA, in 1982, and the Ph.D degree in computer and information science in National Chiao Tung University, Taiwan, in 1998. She joined the projects of C3I System in the Chung Shang Institute of Science and Technology (CSIST) under the Department of Defense, Republic of China, in 1985. She was the head or project manager of the Management Information System, the Secure Intelligent System and the secure system of information warfare of CSIST from 1988 to 1999. Since 2000, she joined Universal Exchange Inc. to establish a secure, reliable trading platform for specific industries.