International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 05 | Aug-2015 www.irjet.net p-ISSN: 2395-0072

Security Management System for Mobile Database Transaction Model using Encryption and Decryption Algorithm

Dr.A.Priya[1]

[1] *Assistant Professor, Department of Computer Science, Thiruvalluvar University College of Arts and Science, Tirupattur, Tamil Nadu, India*

Abstract - *Mobile database is a specialized class of distributed systems. There are security challenges due to the distributed nature of the mobile database application and the hardware constraints of mobile devices. This paper discusses about the security issues that are associated with the database system which are specified in four main operations, such as security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. The rapid development of Information technology has offered many opportunities for integrated business operations. Important security issues for mobile device, mobile operating system and mobile network that maybe affect on mobile database security are discussed along with possible solution. This paper will tackle various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.*

Key Words: *Mobile database security; security vulnerabilities; distributed database, Transaction management, Security*

1. INTRODUCTION

For mobile database systems, security support is even more important to protect the users and devices as well as the database. In mobile communication, since wireless medium is available to all, the attackers can easily access the network and the database becomes more vulnerable for the user and the central computer that located distributed database on it. This paper discusses all the security issues and their solutions in both mobile database system and mobile network. Sorting Database security is a crucial operation that a firm should enhance in order to run its activities smoothly [1] [2]. It is a deliberate effort to protect an organization data against threats such as accidental or intentional loss destruction or misuse. The threats pose a challenge to the organization in terms of integrity of the data and access. The threat can result from intangible loss such as hardware theft or intangible loss such as loss of confidence in the organization activities.

First, security issues divided to four fields that they are important from many aspects.

i. Mobile device,
ii. Operating System on Mobile Device,
iii. Mobile Database and
iv. Mobile Network

The objective of this paper is to conduct a Comprehensive survey on existing security mechanisms and explore disadvantage security of them. The purpose of this document is to provide information to users and organizations on the security capabilities of Worldwide Interoperability for mobile database system and provide recommendations on securing mobile database technologies effectively to users and organizations employing them. Security support is mandatory for any database system. All these activities have been rampant due to electronic commerce as opposed to convectional trade involving physical goods.

2. MOBILE DEVICE AND WINDOWS MOBILE DEVICE SECURITY

Security is an important topic for Windows Mobile Application Developers. Depending on the security configuration of particular devices, applications might need to be signed with either a privileged or unprivileged certificate. Besides signing applications, it is also important to understand the impact of executing applications on 1-tier and 2-tier secure devices [3]. Especially on a 2-tier security configuration, unprivileged and unsigned applications have restricted access to device resources.

Windows Mobile devices Security model summarized as follow:

A. **Application Execution Security**: Applies to code execution. Controls the applications that can run on the device. Controls what applications can do.

B. **Device Configuration Security**: Applies to device management security. Controls that can access to

specific device settings. Controls the level of access to device settings.

C. **Remote Access Security**: Remote API (RAPI) control through ActiveSync. Controls what desktop applications can do on the device.

2.1. Application Execution Security

Depending on the security configuration of a particular Windows Mobile device, applications might be allowed to run or might be blocked from execution on the device [4]. The following application execution permissions are defined for Windows Mobile devices:

i. **Privileged:** The application can do everything on the device, has full write access to the file system and to the system Registry, and is also allowed to install certificates that might allow other applications to run on a particular Windows Mobile device.
ii. **Normal:** The application is restricted in its execution; it cannot call trusted Win32 APIs, write to protected areas of the Registry, write to system files, or install certificates.
iii. **Blocked:** The application is not allowed to execute at all.

Different access levels determine what an unsigned application is allowed to do on a Windows Mobile device. These different access levels are called tiers [6]. The security policy of a particular device determines just how that particular device handles the issues of application signatures and permissions.

i. The first part of the security policy is the device security tiers; devices can have one-tier or two-tier security.

   a. A device with one-tier security focuses only on whether an application is signed; there is no concept of permission restrictions in one-tier security. Under one-tier security, any running application can call any API, modify any part of the file system and modify any part of the registry. One-tier security only restricts application startup. Signed applications can execute with no further checks; unsigned applications require further policy checks to determine if they can run.
   b. Two-tier security restricts both application startup and application run-time permissions. On a device with two-tier security, signed applications can execute with no further checks, unsigned applications require further policy checks to determine if they can run. At run-time, two-tier security restricts an application's access to the APIs, registry, and file system based on the permissions associated with the certificate the application is signed with [5]. Applications signed with a certificate from the privilege certificate store execute with privileged permissions, all other applications run with normal permissions.

ii. The next two parts of the security policy are closely tied together: whether unsigned applications can execute and whether the user should be prompted before the unsigned application executes These four security settings create four common security policies:

   a. Security off: In this policy unsigned applications are allowed to run without prompting the user. The security off policy is a one-tier policy. The security off policy is the default configuration. A device configured with the security off policy is extremely venerable because the device can install malicious applications without your knowledge and those applications have unrestricted access to the device.
   b. One-tier prompt: This policy allows signed applications to execute; the device prompts the user before executing unsigned applications. Once an application is executing, it has no restriction on permissions. This is true for both signed and unsigned applications.
   c. Two-tier prompt: This policy allows signed applications to execute; the device prompts the user before executing unsigned applications. If the user allows an unsigned application to execute, the application executes with normal permissions. Signed application executes with normal or privileged permissions.
   d. Mobile2Market locked: Applications that are signed can execute; users are not prompted to execute unsigned applications. These unsigned applications simply cannot execute. Once the application is executing, the permissions are determined by whether the application is signed with a certificate from the privileged certificate store or the normal certificate store.

The security policy settings are stored in the secure part of the device registry. Without persistent storage, if the Windows Mobile device's battery dies, settings revert to the default security settings in ROM when the device is powered again [7]. With persistent storage, if the Windows Mobile device's battery dies, then the security settings will remain unchanged when the device is powered again. When the device is cold booted manually by the user, the persistent store and all programs and user data is erased, reverting to what was flashed into ROM.

2.2. Device Configuration Security

Device-level security involves managing who has access to a device and its data, controlling which applications can run on the device, and establishing how data is transmitted to and from the device. User access is managed through a PIN or password authentication [8]. A device can be set to lock automatically after a period of inactivity or after being turned off, requiring a user to unlock the device again to use it .

2.3. Remote Access Security

i. Set the RAPI policy to restricted mode whenever other security policies restrict access to the device.
ii. Prompt the user before running normal applications. Microsoft highly recommended that you keep the User Prompt mode on for unsigned application for all Windows Mobile devices.
iii. Assign unsigned themes with a security role of User Unauthenticated. Microsoft highly recommends that you keep the Unsigned Theme policy the SECROLE_USER_UNAUTH security role. This is the default setting.
iv. Keep your Bluetooth off.
v. Users can enable Mobile Encryption through the Encryption Control Panel Application (CPA) which is available on under Settings.
vi. Devices corrupt deleted information on memory cards to prevent access to it.

3. THE SECURITY MANAGEMENT MODEL

The architecture of Multi Check-out Timestamp Order (MCTO) model consists of one base station BS and more than one mobile host MH in the Mobile Network (MN), which communicate with the BS through wireless network as illustrated in Figure 1. The main idea of this model is that transaction execution can be done at the BS and MHs. Transactions at a MH can update data locally and then pre-commit. When the MH connects to the BS, these precommitted transactions are sent to the BS and re-executed as base transactions (BT). BTs are serialized on the master copy of the data stored at the BS. This will result in data consistency [9]. The main advantages of this model are recovered all the weakness of the transactions management models above but the disadvantage of this model, the data is always transferred without security. The proposed model is going to build new security for insecurity data transaction by a using new cipher algorithm.

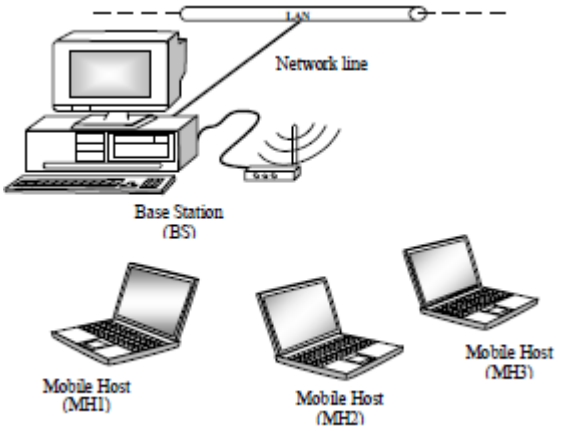


Figure 1: System architecture for the MCTO model

The security management model will extend to work by increase security for the amount *di* will be transfer from the BS to the MH(s) and vies versa, it consists of both encryption and decryption algorithms that are located at the BS and the MH(s) as shown in Figure 2. The encryption algorithm is started when the data transferred. The decryption algorithm is started when encrypted data is received.

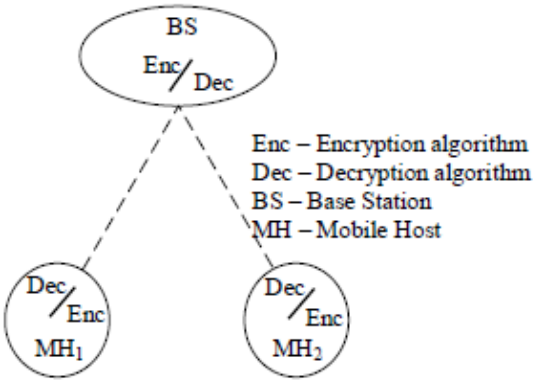


Figure 2: Simple architecture of the proposed model.

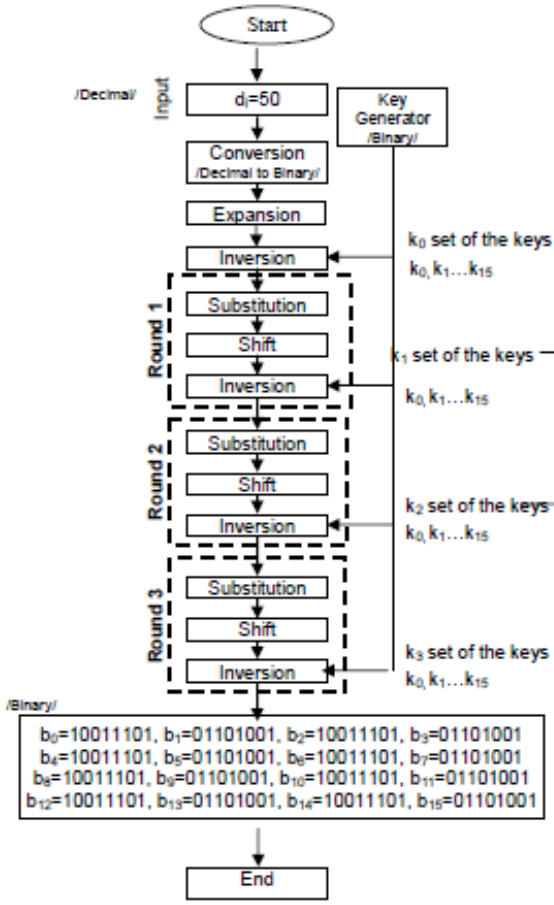


Figure 3.a: Schema for the Encryption algorithm

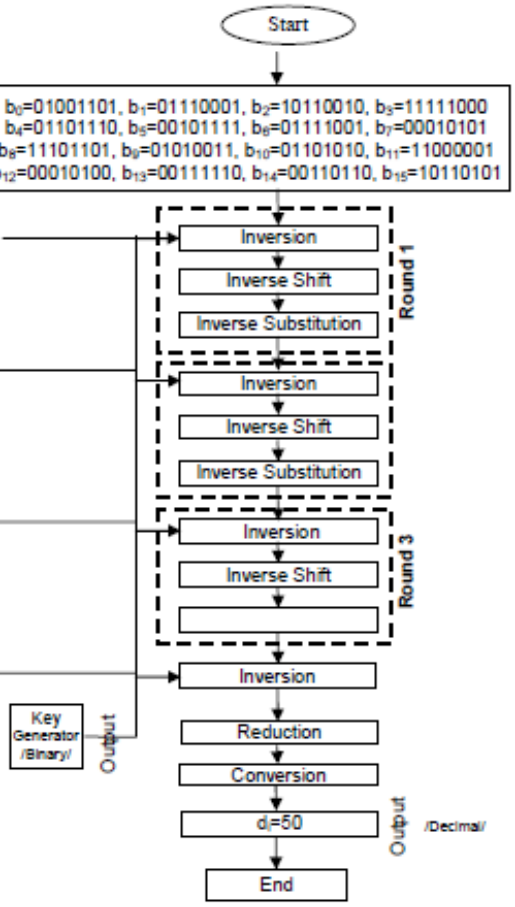
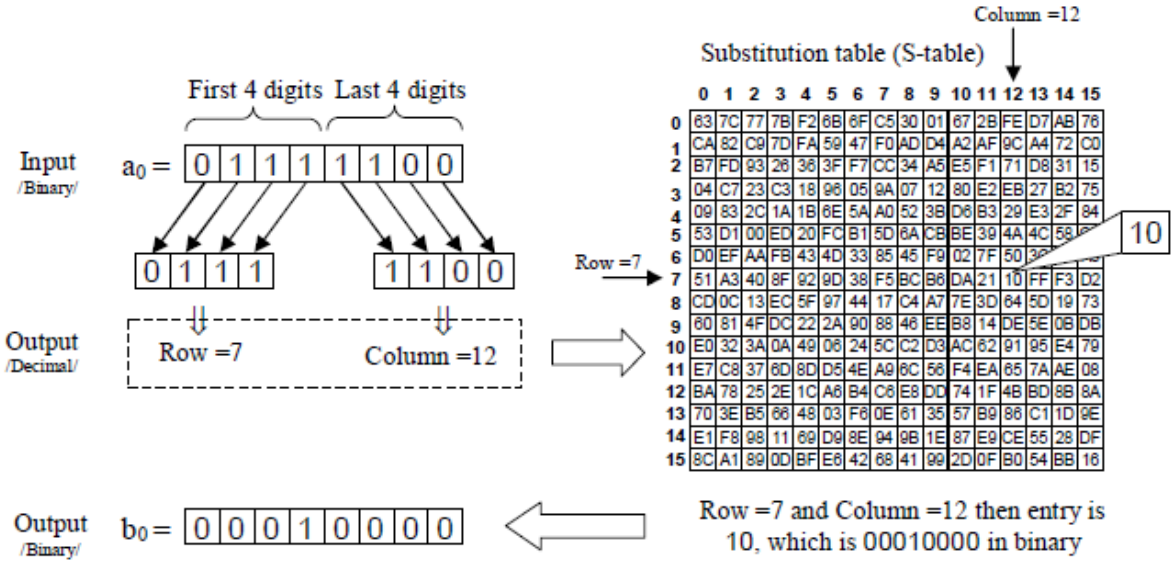


Figure 3.b Schema for the Decryption algorithm



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5D	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
10	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
11	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
12	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
13	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
14	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
15	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 4: Example for Substitution

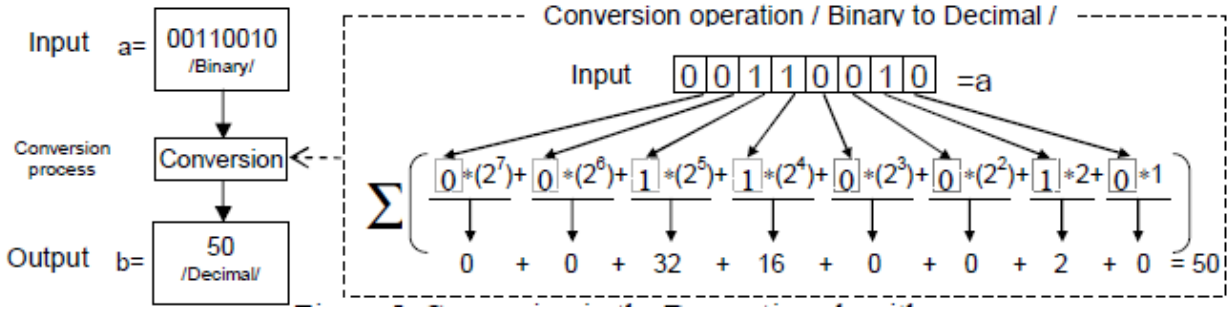


Figure 5: Conversion in the Decryption algorithm.

3.1. Encryption Algorithm

The using notion of crypto algorithm, which is classified in symmetric key cryptography, is designed to security data transaction in mobile network for MCTO model. Both the encryption and the decryption algorithms are used at the BS and the MH(s). The Encryption algorithm, which is used to encrypt data, includes Conversion, Expansion, Mix, Separation and Inversion with three rounds; each round consists of Inverse, Substitute and Shift operations as shown in Figure 3.a.

The Conversion operation in the encryption, which is used to convert decimal data to binary data by a using conversion technique, the Expansion operation in the encryption is used to expand the input 8 bits input data to the sixteen 8 bits output data, the Inversion operation in encryption is started that input data (a0…a15) are combined with a set of keys data (k0…k15) to another output data (b0…b15) one by one bye XOR operation [10].

After the Inversion, the first round of encryption is started. For the first round, the Substitute operation in the encryption is that an input data a0… a15 are substituted to another output data b0… b15 by Substitution table (S-table) as shown in Figure 4. For the 2nd and the 3rd round will be the same of the 1st round. Next the Shift operation in the encryption is started. The Shift operation is used to shift first 3 digits of the input data a1 to the left side by cyclical movement

3.2. Decryption Algorithm

The proposed Decryption algorithm, which is used to decrypt encrypting data, is operated when encrypting data is received. The algorithm consists of three rounds, Inversion, Reduction and Conversion as shown in Figure 3.b. Each round has Inversion, Inverse shift and Inverse Substitution operation layers. The Inversion operation in the decryption is same with previous inversion in the encryption algorithm, and it is used to inverse input 8 bits data and to combine 8 bit input data ai to another output 8 bit data bi in binary by a generated key ki in binary.

For the decryption, the Inversion operation in first round is started and operates that input data (a0…a15) are combined with key data (k0…k15) to another output data (b0…b15) one by one and XOR operation. The keys (k0…k15), which are replicated from the keys (k0…k15) in the encryption algorithm and sent to the receiver (BS or MH) by secure channel. The key (ki), which is used to inverse digit of input data ai in binary, controls the security operation of the Encryption and Decryption algorithm [11]. When the encrypted data is received, the inversion operations are first started and operated on the encrypted data.

Inverse operation in decryption is used to invert digits of the input data ai in binary to another output data bi in binary by XOR operation. After the Inverse operation, the shift operation is used to shift digits of the input data. When the operation is started, last 3 digits of the input data ai is shifted to the right side cyclically [12]. After the shift operation, It would be Substitution operation continued and finish the first round in decryption. The Substitution operation in first round is continued after Inversion in second round and performs that input data (a0…a15) are substituted to the output data (b0…b15) one by one and a using Inverse Substitution table Inv.S-table.

The same thins will done for the 2nd and the 3rd round. The Substitution operation in last round substitutes input data ai to another output data bi by a using Inverse Substitution table. After the Substitution, all round's operation is completed, and Inverse operation continued. The Inverse operation is same with previous Inverse operations that combine input data ai with key data ki to another output data bi by XOR operation [13] [14]. The reduction operation, which is used to reduce digits of input data ai0…a15 in binary, is that input two 8 bit data ai…a15 are reduced to output one 8 bit data "b".

Once reduced the data b it is converted from Binary to the Decimal numeral system by a using technique as shown in Figure 5. The Conversion operation is final operation at the decryption and used to convert input data "a" in binary to output data "b" in decimal. For instance, input data "a" in binary, each digit of the data is multiplied and summarized by 20…27. The function is used to convert only 8 bits in binary data to decimal data [15]. After the conversion in the decryption is finished, while the data di are ready used to work at the place which, located data. Once decrypting data *di* can work as initial usual data *di*.

4. CONCLUSION

In this paper, the Encryption and Decryption algorithm to be secured data transmission between the base station BS and the mobile host MH(s) and to ensure our database at the consistency level once the data are secure. The aim of this paper to made balance between minimum time requesting for any transaction management to avoid the abort transactions and maximum time need to avoid any hacker decryption. We have adapted algorithm in both side (the BS and MH(s) sides) to save the transaction during the transmission between the BS and MH(s).

5. REFERENCES

[1] A.Priya and R.Dhanapal. 2013. "Evaluating the Query for a Mobile Database System through Dongle Transaction Model", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3,Issue 10,October 2013, pp. no.879-887.

[2] A.Priya and R.Dhanapal. 2012. "A Method of Implementing Dongle Transaction Model in Mobile Transaction Systems using Mobile Agents",European Journal of Scientific Research,Vol. 90 No 4 November 2012, pp. no. 536-549.

[3] Forouzan. B. 2007. "Data Communications and Networking", Fourth edition, Mc Graw Hill, Singapore, ISBN 007- 125442-0.

[4] Abdul-Mehdi.Z and Hason.N. 2006. "Trusted Based Diagonal Replication on Grid Database", International conference For Business, Law and Technology, Copenhagen- Denmark, 5-7 December, Vol.2, p.p 441.

[5] Lubinski. A. 1999. "Adaptation Concepts for Mobile Database Security" University of Rostock, Rostock, Germany.

[6] M.H. Dunham and V. Kumar, "Location dependent data and its management in mobile databases," in Int. DEXA Workshop on Mobility in Databases and Distributed Systems, Vienna, Austria, Aug. 1998.

[7] Can Turker and Gabriele Zini, "A Survey of Academic and Commercial Approaches to Transaction Support in Mobile Computing Environments", Swiss Federal Institute of Technology Zurich Institute of Information Systems, ETH Zentrum, Techniqual report #429,NOV 2003.

[8] Notorgiacomo. L. 1994. "Architecture for MLS database management System" Information Security: An integrated Collection of Essays. Essay 19.

[9] M. H. Dunham and V. Kumar. Impact of Mobility on Transaction Management. In Proc. of the ACM Int. Workshop on Data Engineering for Wireless and Mobile Access, August 20, 1999, Seattle, WA, USA, pages 14–21, ACM Press, 1999.

[10] J. Gray, P. Helland, P. O'Neil, and D. Shasha, "The dangers of replication and a solution," in ACM SIGMOD Conference, Montreal, Canada, June 1996.

[11] Abdul-Mehdi, Z.T. Mamat, A.B. Ibrahim, H. Dirs, Mustafa.M. 2006."Multi-Check-Out Timestamp Order Technique (MCTO) for Planned Disconnections in Mobile Database", The *2nd* IEEE International Conference on Information & Communication Technologies*: from Theory toApplications* , 24-28 April, Damascus, Syria,Vol.1, p.p 491-498.

[12] Abdul-Mehdi.Z.T, Mamat.A, Ibrahim.H and Deris.M. 2006. "Transaction Management Model for Mobile Databases". Phd Thesis in Computer Science, Faculty of Computer Science and Information Technology, Univesrity Putra Malaysia, P.P.3.

[13] Daniel Barbará "Certification Reports: Supporting Transactions in Wireless Systems". In ICDCS, 1997.

[14] J.Holliday, D.Agrawal and A.El Abbadi," Disconnection modes for mobile databases", Journal of Wireless Network, Kluwer,8(2002), pp.391-402.

[15] J.Holliday, D.Agrawal and A.El Abbadi," Epidemic Algorithms for Replicated Databases", IEEE Trans. On Knowledge and Data Engineering, vol.15, 5(2003), pp.1218-1238.

BIOGRAPHIES

A.Priya is received her Ph.D in Computer Science at Bharathiar University, Coimbatore. She got her Master degree in Computer Science and Master of Philosophy in Computer Science in Avinashilingam University, Coimbatore. She is currently working as an Assistant Professor in the Department of Computer Science, Thiruvalluvar University College of Arts and Science, Tirupattur, Tamil Nadu, India. She has 14 years of teaching experience, 8 years of administrative experience and 9 years of research experience. Life time Member in ISTE Chapter. Organized DRDO sponsored National Conference in the Department of Computer Applications, Velammal Engineering College, Chennai. Her publications are four International Journal, two International Conference (in IEEE Proceedings) and eight National Conferences.