International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 12, December 2014 **ISSN 2319 - 4847**

A Review on the role of Encryption in Mobile Database Security

D. Roselin Selvarani[1] and Dr. T. N. Ravi[2]

[1]Department of Computer Science, Holy Cross College, Bharathidasan University, Tamil Nadu, India.

[2]Department of Computer Science, Periyar E.V.R. College, Bharathidasan University, Tamil Nadu, India.

ABSTRACT

Data-driven applications are realized due to the powerful lightweight computing devices such as Smart phones, Laptops, Tablets and low cost mobile connectivity. Today more and more businesses move toward employees' mobility. While the employee moves, along with him the mobile device as well as the database stored in the mobile device also moves. Therefore security of the mobile database is an important issue to be considered. It is highly critical because of the sensitivity and significance of data stored in the device. The main objective of the database security is the protection of data against accidental or intentional loss. Security approaches based on encryption play a vital role in securing mobile database. The need for encryption is strongly recommended to mitigate the risk of intentional or accidental disclosure of sensitive data in portable devices. Among the symmetric and asymmetric encryption algorithms, asymmetric encryption is highly computationally intensive compared to symmetric encryption. Therefore, for resource constraint mobile devices, symmetric key algorithms are more suitable. The main objective of this paper is to review the various Encryption algorithms used in mobile database security.

Keywords:- Mobile database Security, Encryption, Symmetric key, Asymmetric key, Secured Architecture for Mobile database

1. INTRODUCTION

The usage of smart phones around the world exceeded 1 billion in 2012 and it is expected that the next billion devices could be reached within another three years [1]. Such powerful lightweight computing devices and less cost mobile connectivity paved the way for data-driven applications in mobile environment. To access any data, anywhere, anytime is possible due to Mobile data-driven applications. Therefore the fame of Mobile database is also increasing drastically. A mobile database 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 items such as customer id, customer name, phone number. One of the key characteristics of the mobile database systems is their ability to deal with disconnection. A Mobile database is a portable database and physically separate from the corporate database server, but is capable of communicating with that corporate database server from remote sites allowing the sharing of corporate data [2]. Confidentiality, Integrity, Authentication, Authorization and Non-repudiation are the fundamental requirements for database security. But as far as Mobile database is considered, along with these basic requirements it has additional risks or challenges due to the mobility of the users, the portability of the hand held devices and wireless links. It may also encounter an array of security problems from the mobile users, hackers and viruses. In order to ensure the security of the mobile database, proper authentication mechanism, suitable access control scheme and strong encryption technique must be implemented. In addition to that audit and recovery procedures must be incorporated. After reviewing the issues of the mobile database from many literatures, it is found that in [3]-[9], the authors have invariably addressed the security and privacy as one of the important critical issues to be considered for any Mobile application which needs Mobile database. So, new algorithms or techniques must be designed for securing Mobile Databases keeping in mind the restrictions of mobile devices such as limited memory capacity, less computation capability and battery power consumption. Security approaches based on encryption play a vital role in securing mobile database. The need for encryption is strongly recommended in [7]-[10], to mitigate the risk of intentional or accidental disclosure of sensitive data in portable devices. Two broader classes of cryptographic algorithms are Symmetric (or Private Key) encryption and Asymmetric (or Public key) encryption. Public key encryption is highly computationally intensive compared to Private key encryption. One of the limitations of mobile device is the limited battery power. Therefore minimizing power consumption is crucial in such type of algorithms. Many factors such as the available memory, hardware architecture, software implementation, etc. have an impact on the power consumption. Therefore, for resource constraint mobile devices, Symmetric key algorithms are more suitable [10]-[11]. In order to ensure the overall security of Mobile database , three different areas need to be addressed such as

Security of the data stored in the mobile device, Security of the Mobile device itself, and the Security of the Mobile Network through which data are sent/received. The issues, solutions and recommendations of the Mobile device security is presented in [12]. Among these three areas encryption plays a major role in two areas such as encrypting the local database, which is stored in the mobile device and encrypting the data that are transmitted between the mobile device and the server using mobile network. The main focus of this paper is to review the mobile database security using encryption found in the literature so far. After reviewing a lot of articles, in this paper we present the state-of-the-art security management in Mobile databases. The rest of this paper is organized as follows: In Section 2, Review of literature is provided for mobile database security using Encryption. In Section 3, Security Architecture of Mobile Database is presented under the various headings such as security of mobile device, security of the mobile database (the content) and the security of the mobile network. In Section 4, the Issues, Solutions and Recommendations of Mobile database is discussed. The paper is concluded in Section 5.

2. REVIEW OF LITERATURE

2.1. Review on Basic Concepts of Mobile Database Security

In [7], the authors presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database. In [8], the authors focused only on the concepts of Mobile Database security. They briefly summarized the basic requirements of mobile database security, mobile device security and mobile network security. They also provided Problems, Security Challenges and Solutions for Mobile Distributed Database. In [9], the authors presented the basic concepts of mobile database and its issues and solutions. Security related strategies and techniques were also provided by them. In [13], the authors presented the overall security of the mobile database application and they explained that it is achieved through securing four different areas such as security for Mobile Device, Central Computer, Communication Link and Application Specific issues. They discussed implementing encryption inside DBMS as well as outside the database. They also provided the security implications of Wireless LANs (WLANs) for mobile applications, and provided security tools and solutions. They also made a comparative study among the various wireless security protocols. In [14], the authors analyzed the security threats and solutions for various mobile devices and compared Android and iOS. They tried to identify threats and dealt with the subject of security in four fields namely Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also briefly explained the threats and the possible solutions.

2.2. Review on Encryption techniques in securing mobile database

In [10], the author provided security consideration for Portable and Removable media devices. He examined the security policies for portable and removable devices and how encryption can help these devices to achieve authentication, auditing and authorization. He also provided a table which contains portable and removable media device encryption software companies, products and federal information processing standards validation. Protecting data from theft or loss due to the use of removable devices, there is a need for encryption software for removable media along with general laptop encryption is needed. The encryption software available now is capable of implementing authorization standards that allow only the copying of designated files onto removable media and encrypting data residing on these devices using AES 128/256 bit encryption automatically. In [15], the author discussed the important requirements for security solutions namely implementing software-base access control and the role of encryption. He provided few measures to be considered for securing mobile systems. One among them is permanent encryption of the hard disk to prevent direct reading. The author also presented another measure in which he stated that Work group can use encryption routine that has its secret from the master password. When this is followed, diskettes that are produced on a computer with such security features can only be read on the same computer equipped with the same encryption module, initialized with the same master password. In [16], the author insisted on storage level encryption, when the sensitivity level of the data stored is minimum. If the level of sensitivity of the data is too high then the company policy should not permit the mobile user to store the data into the device. But whatever may be the level of security of the data it is nice to have the encryption software to secure the data stored in the device. The authors also discussed the various factors to be considered for evaluating handheld devices for corporate standardization. In [17], the authors stated that key exchange and key agreement, encryption and decryption are the important steps needed for secure communication in mobile computing to achieve the vital security factors namely confidentiality, integrity and authentication. The main objective of this paper is to improve the authentication stage of an Elliptic Curve Cryptography (ECC) security algorithm. Due to the smaller key size of ECC, it is more suitable for resource constraint devices compared to Rivest-Shamir-Adleman (RSA) to provide equivalent security. They also found that 163bit ECC key is equivalent to 1024bit RSA key in providing the same level of security. The smaller size of the key supports faster computation, lower power consumption, memory and bandwidth savings which are highly needed for resource constraint mobile devices. They used Elliptic Curve Diffie Hellman (ECDH) method for key exchange. In [18], the authors proposed a new Client-based

security component called Chip-Secured Data Access (C-SDA) that enforces security requirements such as Confidentiality and Authentication in the client. It acts as a mediator between a client and an encrypted database. It is embedded in a smartcard to prevent any tampering that can occur. Hardware and Software combination constitutes a strong guarantee against data attacks. Several attempts have been made to strengthen server based security approaches with database encryption [19]. However, as Oracle confesses, server encryption is not the expected "armor plating" because the Database Administrator (or an intruder usurping his/her identity) has enough privilege to tamper with the encryption mechanism and get the clear text data. In [20], the authors designed a lightweight security mechanism for m-commerce in order to meet the security needs of the lightweight devices, which are highly resource constraint. The main objective of this paper is to design and implement lightweight security mechanism for achieving end-to-end security between the handheld device and the gateway server. In this paper, the proposed mechanism uses simple password authentication and Public key cryptographic mechanism to conduct a secure mobile commerce. A mobile user who wished to conduct e-commerce transaction with m-commerce provider initiates the security mechanism from his/her mobile device. After the successful completion of authenticating the user, symmetric secret key is shared by the mobile device and wireless protocol gateway. The wireless protocol gateway executes complex transaction protocol with the application server efficiently on behalf of the user. The mechanism may be complemented by tamper-resistant hardware device to achieve a restricted form of non-repudiation. The proposed system meets the security requirement of m-commerce and it is suitable for implementation on resource constraint mobile devices. In real deployment environment the above mechanism is proved to be practical. In [21], the authors proposed Authorized Summary Schemas Model, which is an extension of Summary Schemas Model (SSM). SSM is an authorization model for multi-database system in the wired environment and it was extended to support for mobile clients with mobile/stationary databases in a wireless environment. In the proposed model, authentication or secure session setup is provided by password based system, where a user is assigned with username and password. Diffie-Hellman Key Exchange protocol is used for authentication. Advanced Encryption Standard (AES) is used for encrypting the message during data exchange. Confidentiality and integrity is provided through encryption. Non-repudiation in secret key algorithm is possible using Digital Signature. To decide whether a user has sent message, he/she includes digital signature in the message. At the receiver end, digital signature is decrypted using the shared secret key. The authors provided authorization through digital signature using SHA-256 hashing utilities (Symmetric block encryption algorithm). In [22], the authors developed a ubiquitous cryptography called Random number Addressing Cryptography (RAC) and implemented it using the Hardware support called HCgorilla processor. This processor is a single chip multimedia mobile processor followed Hardware / Software co-design to unify sophisticated techniques like strong hardware security, low power, and high throughput. RAC is an innovative common key technique and has more promising performance than block cipher like DES and AES as it does simply memory access without any arithmetic logic operation like XOR used in AES or DES. It scrambles memory access at hardware level as it does not need any complicated operations. Using this algorithm, the data is physically divided and stored in block. A Random Number Generator (RNG) generates a random number and both data blocks and RNG output are synchronized. Thus it makes the memory access scrambled and creates the encryption of plain text. The authors did not present any result related with RAC. In [23], the authors presented the fundamental concepts for achieving data securely by applying data encryption and secret sharing of the encryption key. They introduced key encapsulation mechanism and Threshold cryptography. A threshold cryptography is a form of technology that distributes shares of a private key to a certain number of members. A receiver can obtain the result of decryption or sign by gathering more than a certain number of partial results, which are computed by each member with each share. A member need not use a threshold cryptography to reconstruct the encryption key, once he/she reads the data but can utilize a secret sharing scheme. In [24], the authors presented the Mobile Emergency Triage system which provided doctors with decision support for emergency care by pulling information from a patient's health record and a medical literature database. They also explained how hospitals are now using electronic medical records and computer applications in order to provide more efficient and thorough care for their patients. They used a new encryption technology called Policy-based encryption for providing both encryption and access control. They also proposed an extension to an existing scheme which allows the use of this cryptography in a hospital setting. In [25], the author described the need for encrypting the data stored in handheld devices for efficient mobile workforce. He also stated that the encryption software to secure any data stored on the mobile device falls into the "nice to have" category. In [26], the authors proposed a novel stream cipher scheme, Self encryption**,** to address the challenges encountered by the encryption algorithms for mobile devices. Considering data as a binary bit stream, the authors generated the key stream by extracting n bits in a pseudo random manner based on a seed, which is created through Hash functions with user's unique PIN and a nonce as inputs. At the server side, the self encryption protocol supports two working models namely Normal model and emergent model. Normal model consists of the working flow when the mobile device is used normally by the legitimate users, whereas the emergent model is triggered when a mobile device is reported lost. The proposed self encryption stream cipher is Hardware oriented and aims at light weighted design. In this algorithm the bit stream and key stream are stored separately so that even the person who has the knowledge of encryption algorithm cannot recover the original data from the cipher text. Moreover the length of the key stream is not fixed in this algorithm, which makes it impossible to find out the original data

through Brute force attacks. In [27], the authors discussed the security policy of mobile databases and presented the various safety measurements to solve the problems. To ensure the safety of mobile database they suggested few mechanisms such as authentication, encryption, auditing, backup and recovery. The authors proposed the use of Elliptic Curve Cryptography as well as the Triple encryption authentication of the class of Kerberos for database encryption to strengthen the encryption of database. In [28], the author proposed a Paradigm for securing Mobile Database and identified three areas to be secured such as Client side security, Server side security and Security during data transmission. She recommended AES for encrypting local database on the mobile device and Public key algorithm for data transmission over network. In [29], the authors presented a block cipher based symmetric encryption scheme, particularly intended for resource constrained devices called Scalable Encryption Algorithm (SEA**)**. It is a low computational cipher scheme with miniaturized code size, memory and power, developed for processors with a restricted instruction set. SEA is parametric with plain-text, key and microprocessor size, and found to be powerful with the grouping of encipherment or decipherment and derivation of the keys. It suits all the platforms. As it operates on limited resource processor, it can do only few basic operations such as XOR, AND, OR, mod 2^b addition . It was meant for software implementations in microcontrollers, smart cards and small embedded systems. In [30], the authors proposed a new Improved SEA which is applicable in the scenario where there are limited processing resources and throughput requirements. They offered low-cost encryption routines (with small code size and memory) targeted for processors with a limited instruction set such as AND, OR, XOR gates, word rotation and modular addition. The proposed design is parametric in the text, key and processor size, provided to be secured against linear or differential cryptanalysis, allows efficient combination of encryption/decryption and on-the-fly key derivation. It has advantages such as the low cost performances, full flexibility for any parameter of the scalable encryption algorithm using Very High Speed Integrated Chip Hardware Description Language coding. In [31], the authors introduced a generic architecture for Partial encryption scheme for low-power mobile devices. The main objective of this paper is to design downloadable and real-time streaming contents, and also to facilitate a trade-off between minimizing the encryption/decryption overhead and provide sufficient digital rights management (DRM) security for the service provider. The proposed scheme was evaluated by applying it to real-world multimedia contents. The results indicated that encrypting only a small portion of video content can effectively impose DRM restriction on the content which reduces the decryption overhead on low-power mobile devices.

3. SECURED ARCHITECTURE FOR MOBILE DATABASE

Figure1 represents the Architecture for Mobile database security. Mobile database security is focused on three different areas such as Security of Mobile Device, Security of Mobile Database (the content) and Security of Mobile Network. Among these three areas Encryption is mainly used both in securing the mobile database as well as the mobile network.

3.1. Security of Mobile Device

Consider a Mobile Worker proceeds for business along with his mobile device away from his corporate. Due to the mobility and portability, there is a lot of possibilities of device theft or loss. Once the device is lost, the significant data stored inside is also lost. Therefore careful security related measures should be adopted to protect the device as well as the data. The important mobile device threats are loss or theft of mobile devices, interception of data when it passes over 3G networks/WiFi/WiMAX, capturing of data through Bluetooth connections and mobile viruses. The issues on mobile devices can be grouped into 3 categories namely Physical Issues, Logical Issues, and Network Issues. The physical issues are Loss/theft of mobile devices, poor or no device authentication, problems due to secondary storage devices. Break-in attack, attack on mobile OS, confidentiality of the data resides inside and authentication are some of the logical issues. The network threats are due to mobile viruses or worms, over billing attacks, Botnet attacks, Infrastructure attacks, wireless attacks and denial of service attacks. In addition to these issues in paper[12], Personnel issues such as BYOD and Insiders attacks were also discussed elaborately by the authors. The degree of security needed for the mobile device depends on the level of access to the corporate intranet as well as the level of sensitivity of the data it contains[16].

3.2. Security of Mobile Database

The security of mobile database is mandatory as it has sensitive and significant data. Encryption plays a major role in protecting such sensitive data. Today many organizations are going mobile and they permit the mobile workers to carry their sensitive data outside the physical boundaries for transaction. Due to this there is a possibility of data getting exposed to outsiders including competitors. Therefore security is a major concern for such type of organization. Along with the fundamental requirements for database security such as Confidentiality, Integrity, Authentication, Authorization and Non-repudiation, Mobile database has additional risks or challenges due to the mobility of the users, the portability of the hand held devices and wireless links. It may also encounter an array of security problems from the mobile users, hackers and viruses. In order to ensure the security of the mobile database, proper authentication mechanism, suitable access control scheme and strong encryption technique must be implemented. In addition to that

audit and recovery procedures must be incorporated. To maintain the confidentiality of the data Encryption is the only option.

3.3. Security of Mobile Network

Mobile database that resides inside the mobile device need to be synchronized with the server at a particular point of time (after a transaction is completed or at the end of the day). Secured Network path is needed to transmit the mobile data from

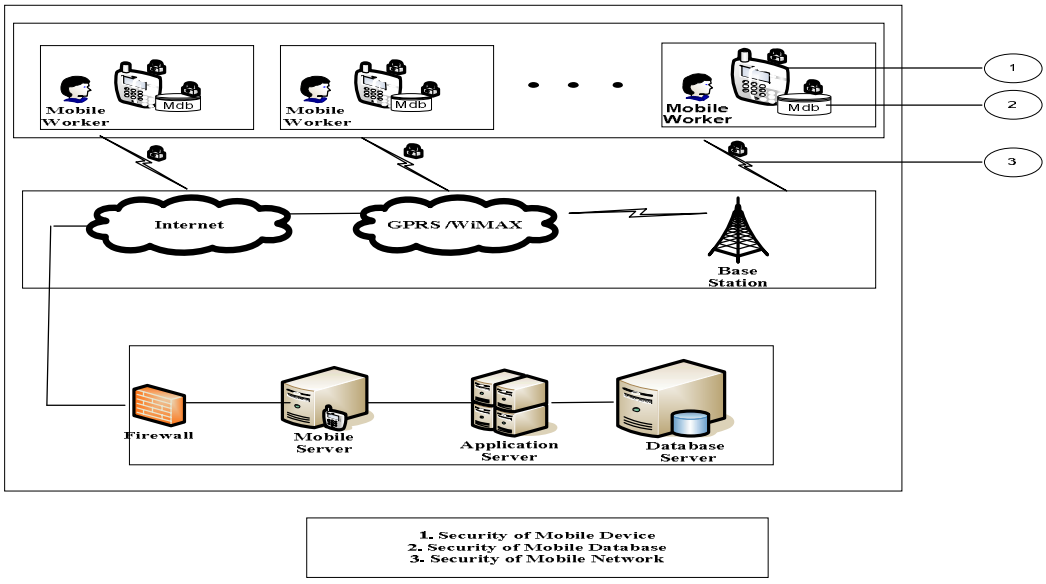

Figure 1 Architecture for Mobile Database Security

the mobile client to the server. There are many possible attacks from Viruses, Worms, Trojans, SMS and MMS spam. DoS attack in one in which even the legitimate users are not able to utilize the services. SYN flood, Over billing attack, application layer attack, signaling level attacks are some of the possible attacks on Mobile networks. The various types of attacks, target and the purpose of attacks along with possible solutions were clearly explained in [7], [8].

4. ISSUES, SOLUTIONS AND RECOMMENDATIONS FOR MOBILE DATABASE SECURITY

The Table 1 represents a list of issues, solutions and recommendations for Mobile database security.

Table 1: Issues, Solutions and Recommendations for Mobile database Security

2. Unauthorized access of the data (Authentication)	Password / PIN / Token / Biometric factors like Fingerprint, Iris recognition, Voice recognition etc.	Ensure that proper Authentication mechanism is incorporated to determine and verify the user's identity
3. Unauthorized modification of the data (Integrity)	1. Grant / Revoke command 2. MAC / DAC / RAC (Mandatory/Discretionary/ Role based access Control) in case of Multi level security	Ensure that appropriate Access Control mechanisms are established to protect data integrity by restricting who can alter data
4. Destruction of Sensitive data due to the device corruption	Backup / Recovery procedure	Ensure that periodic backups of mobile devices are done so that it can be quickly put into use again whenever any destruction occurs

5. Unauthorized disclosure of data due to device lost/theft (Device Lost)	1. PIN/Password/Pass code/pass pattern 2.Remote Wiping	1. Ensure that mobile device has Lockout facility so that when an unauthorized person tries to enter PIN/Password/ Pass code unsuccessfully for more than 5 times, the device will automatically lock out. 2. Whenever the device is lost/theft immediately inform it to the organization, so that data stored inside device can be deleted through Remote wiping.
6. Interception of data through WiFi, Bluetooth etc.	Turn off Bluetooth and WiFi facilities.	Ensure that Bluetooth, WiFi enabled mobile devices are turned off when they are not used.
7.Unauthorized access modification of the data during transmission	1.**Encryption** 2.Server Authentication and Client Authentication 3.WPKI Certificate	Ensure that the network path is secured between Mobile Client and the Server.

5. CONCLUSION

In this paper, review on the Security of Mobile database using Encryption algorithms is done elaborately. Recently many papers have been published on Mobile database security review but our paper focuses on the role on Encryption on mobile database security. Encryption technique is mandatory for mobile database security in two important situations: when the database is stored inside the mobile device(local database) and when the database is transmitted between the mobile client and the server. Many light weight algorithms are also found in the literature. But it is a challenge for a researcher to design a new encryption algorithm which may perform better than the existing algorithms in terms of not only less Encryption and decryption time but also to meet the limitations of resource constraint mobile devices.

REFERENCES

[1] Anshul Srivastava, "2 Billion Smatphone Users by 2015: 83% of Internet usage from Mobiles [Study]", January 23, 2014. [Online], Available : http://www.dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017/#ixzz3FNSkxDMH , [Accessed : Sep. 5, 2014].

[2] IAMR Group of Institutions, "Security in Mobile Database Systems", Para1, May 28, 2011. [Online], Available : http://iamrgroupofinstitutions.blogspot.in/2011/05/security-in-mobile-database-systems.html , [Accessed : Sep. 5, 2014].

[3] EPFL, U. Grenoble, INRIA-Nancy, INT-Evry, U. Montpellier, U. Paris, U. Versailles, "Mobile Databases: a Selection of Open Issues and Research Directions", SIGMOD Record, Vol. 33, No. 2, June 2004.

[4] Darin Chan and F. John Roddick, "Summarisation for Mobile databases", Journal of Research and Practice in Information Technology", Vol. 37, No.3, pp.267-284, August 2005.

[5] D. Weider Yu, Tamseela Amjad, Himani Goel and Tanakom Talawat, "An Approach of Mobile Database Design methodology for Mobile Software Solutions", The 3rd International Conference on Grid and Pervasive Computing - Workshops, IEEE, 2008.

[6] A. Sripriya, Dr. R. Dhanapal, "A Cache Operation in Mobile Database Using Genetic Algorithm", International Journal of Recent Trends in Engineering, Vol. 2, No. 4, November 2009.

[7] Parviz Ghorbanzadeh, Aytak shaddeli, Roghieh Malekzadeh, Zoleikha Jahanbakhsh, "A Survey of Mobile Database Security Threats and Solutions for It", 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), pp.676-682, 2010.

[8] Tao Zhang, Shi Xing-jun, "Status Quo and Prospect on Mobile Database Security", Telkomnika, Vol. 11, No. 9, pp. 4949-4955, September 2013.

[9] A.R. Bhagat, V.B. Bhagat, "Mobile Database Review and Security Aspects", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, pp. 1174-1182, March 2014.

[10] Faith M. Heikkila, "Encryption : Security Considerations for Portable Media Devices", IEEE Security and Privacy , 2007.

[11] Ruangchaijchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs", The Third IEEE workshop on Wireless LANS, September 27-28, 2001.

[12] D. Roselin Selvarani and Dr. T. N. Ravi, "Issues, Solutions and Recommendations for Mobile Device Security", International Journal of Innovative Research in Technology and Science (IJIRTS), ISSN : 2321- 1156, Vol.1, No. 5, pp. 9-14, November 2013. (Online) http://ijirts.org/volume1issue5/IJIRTSV1I5027.pdf

[13] Sanket Dash, Malaya Jena, "In the Annals of Mobile Database Security" CPMR-Interntional Journal of Technology, Volume 1, No. 1, December 2011.

[14] Hezal Lopes, Rahul Lopes, "Comparative Analysis of Mobile Security Threats And Solution", Int. Journal of Engineering Research and Applications www.ijera.com Vol. 3, Issue 5, pp. 499-502, Sep-Oct 2013.

[15] M.A. Badamas, "Mobile Computer Systems - Security Considerations", Information Management & Computer Security, MCB University Press, pp.134 – 136, 2001.

[16] Wesley Chou, *Cisco Systems* , "Considerations for an Efficient Mobile Workforce", Wireless Broadband Technologies ,IEEE, Computer Society, 2008.

[17] Janet Light, Deepika David, "An efficient Algorithm in Mobile computing for Resource Constrained Mobile devices", ACM, 113-114, 2008.

[18] Luc Bouganim, Philippe Pucheral, "Chip-Secured Data Access: Confidential Data on Untrusted Servers", Proceedings of the 28th VLDB Conference, Hong Kong, China, 2002.

[19] Oracle Corp., "Advanced Security Administrator's Guide", Release2, (9.2), 2002.

[20] Kwok- Yan lam, Siu-Leung Chung, Ming Gu, Jia-Guang Sun, " Lightweight Security for Mobile Commerce Transactions", Computer Communications, Elsevier Publications , Vol. 26, pp. 2052-2060, 2003.

[21] Harshal Haridas, Ali R. Hurson, and Yu Jiao, " Security Aspects of Wireless Heterogeneous Databases - Protocol, Performance, and Energy Analysis", In Proceedings of the International Conference on Parallel Processing Workshops (ICPPW'03), IEEE, 2003.

[22] Masa-aki Fukase, Tomoaki Satot, "Innovative Ubiquitous Cryptography and Sophisticated Implementation", pp. 364-369, ISCIT 2006, IEEE, 2006.

[23] Takashi Matsunaka, Takayuki Warabino and Yoji Kishi, "Secure Data Sharing in Mobile Environments", In the Proceeding of the 9th International Conference on Mobile Data Management, IEEE Computer Society, 2008.

[24] Kathryn Garson, Carlisle Adams, "Security and Privacy System Architecture for an e-Hospital Environment", ACM, 2008.

[25] Wesley Chou, "Considerations for an Efficient Mobile Workforce", Wireless Broadband Technologies, IEEE, Computer Society, 2008.

[26] Yu Chen and Wei-Shinn Ku, "Self-Encryption Scheme for Data Security in mobile Devices", CCNC'09, Los Vegas, NV, USA, 2009.

[27] Huaixiang Wang, DeyuDang, Shi Min, "The Analysis of the Security Strategy of Embedded Mobile Database", pp. 476-478, IEEE, 2010.

[28] D. Roselin Selvarani, "A Secured Paradigm for Mobile Databases", N. Meghanathan et al. (Eds.), Proceedings of 3rd International Conference on Recent Trends in Network Security and Applications (CNSA 2010), Springer Communications in Computer and Information Science 89, ISBN 978-3-642-14477-6, ISSN 1865-0929, Springer-Verlag Berlin Heidelberg, pp. 164–171, 2010.

[29] J. Jegadish Kumar, S. Salivahanan, K. Chenna Kesava Reddy, "Implementation of Low Power Scalable Encryption Algorithm", International Journal of Computer Applications, Volume 11, No.1, pp. 14-19, 2010.

[30] B. Praveen Kumar, P. Ezhumalai, P. Ramesh, Dr. S. Sankara Gomathi , Dr . P. Sakthivel, "Improving the Performance of a Scalable Encryption Algorithm (SEA) using FPGA", International Journal of Computer Science and Network Security, Vol.10, No.2, February 2010.

[31] Eun Su Jeong, Bum Han Kim, Dong Hoon Lee, "A generic partial encryption scheme for low-power mobile devices", Springer Science+Business Media, New York, 2013.

AUTHORS

Dr. T.N. Ravi, born on 01.06.1964, has started his teaching career in the year 1985. Currently, he is working as Assistant Professor of Computer Science, Periyar E.V.R. College (Autonomous), an institution run by the Director of Collegiate Education, Government of Tamil Nadu, India. He is basically a Mathematics Graduate, completed both Under Graduation and Post Graduation. He has completed B.Ed., in Mathematics, P.G.D.C.A., and then completed M.Sc. & M.Phil. in Computer Science. He has successfully completed his Ph.D. in Computer Science in the year 2010. He pursued his research in

the area of Parallel Computing and also did real time testing at National Aerospace Laboratories, Bangalore, India. His research interests are Parallel Processing, Grid Computing, Genetic Algorithms, Artificial Intelligence and Data Mining. He has published 17 research articles in International / National Journals. He has delivered about 30 invited talks at State Level and National Level Conferences. He acted as Chair for several Conferences at State and National Level. He has rendered his academic services to various Institutions, Universities within and outside Tamil Nadu, Service Commission etc

Ms. D. Roselin Selvarani is working as Asst. Prof. of Computer Science department at Holy Cross College(Autonomous), Tiruchirappalli affiliated to Bharathidasan University. Her research interests include Mobile database, Mobile Networks, Mobile and Pervasive Computing. She is currently a Research Scholar at Bharathiar University. She has presented 16 papers in National and International Conferences and published few papers in referred International Journals.