Reliable and Fault Tolerant Mobile Transaction Paradigm using Surrogate Object

Ravimaran S., Kanimozhi G., and Maluk Mohamed M. A.

***Abstract*—Today vast practical expansion in mobile technology have possibly allowed service consumer and service providers to replace the traditional transaction process into Mobile transaction process. Due to the various challenges in the both traditional and distributed transaction systems, the advanced Mobile Transaction process yields several benefits and flexibility to both consumer and provider. However, more critical issues have not yet fully deal with in mobile transaction system, mainly because of security concern. This paper propose a reliable and fault tolerant Mobile Transaction paradigm using surrogate object which provides a text based as well as biometric authentication which has finger print and face recognition for strong authentication and utilizes cryptographic method for securing the Mobile transaction process. And moreover, efficient fault tolerance mechanism which helps in case of the mobile device gets switch off or any network connectivity issues occurs, to provide an optimal mobile transaction process to an authorized user with increased reliability, that can be done by using this surrogate object model. This new approach is evaluated through simulation and it shows the proposed system is more reliable and secured than the existing Mobile transaction process.**

***Index Terms*—Authentication, Biometrics, Cryptography, Integrity, Mobile Transaction, Reliable.**

I. Introduction

The implementation of internet into mobile devices, with the combination of these two, the ever-present connectivity has become a reality. The opportunity that mobile phones offer has pulled more people into the wireless world, and also more citizen-related services are offered via mobile devices. Year after year mobile devices, primary used for voice communication, have been included in improving health system, transportation, governance, public safety, enterprises etc. It has been realized that mobile technology is crucial to finding solutions to some of the world‘s greatest challenges. As the number of mobiles has grown in many times, it is difficult to measure the amount of change that mobile phones have made in the social and economic spheres. Private sector applied mobile technology in its work much earlier than the public sector. The importance of an improved mobile transaction system is beneficial to both service provider and consumer. In general, mobile transaction system must meet the principles and requirements for any applications such as mobile voting, mobile banking etc., Due to the resource limitations in mobile environment; mobile transaction process has more challenges than the traditional transaction process in term of performance and security. A transaction scheme must protect the privacy and integrity of the consumer data. For example, Consider an application E-election transaction scheme has typical requirements include, Completeness: All valid votes must be counted correctly. Soundness: Dishonest voters cannot disrupt the voting process. Privacy: All ballots must be secret. Unreusability: No voter can cast his ballot more than once. Eligibility: Only those who are allowed to vote can vote. Verifiability: Nobody can falsify the result of the voting process. Fairness - Nothing must affect the voting.

In this paper we propose a reliable and fault tolerant Mobile Transaction paradigm using surrogate object, which provides the text based as well as biometric authentication which has face recognition and finger print for strong authentication and utilizes cryptographic method for securing the transaction information to avoid fraud. In our mobile transaction process, the data transferred from mobile devices to the database server via surrogate object is secured by cryptographic method in terms of key size. The factors such as computing performance, confidentiality, integrity and anonymity are useful to meet the mobile transaction successfully. This can be done with the help of WAP mobile phone which is camera equipped with internet connectivity and the transaction application installed. And moreover, efficient fault tolerance mechanism is proposed for optimal mobile transaction process to an authorized user with increased reliability by using surrogate object model. Our security scheme needs low computation complexity in portable communication devices. Hence this new approach provides better performance and connectivity.

The rest of this paper is organized as follows; Section 2 describes background and related work, Section 3 explains about proposed system, Section 4 shows performance evaluation and finally Section 5 gives conclusion of this paper.

II. Background Related work

Today, mobile phones are used for much more than just for communications. They are provided with a rich service plan, to offers a wide spectrum of mobile functions and services, including personal data management, entertainment capabilities (such as digital games and music), mobile messaging, and location-based peer-to-peer applications, secure mobile payment and advertising services. The strong demand of mobile applications and services raised increasing concerns on the security for mobile accesses, user privacy, and mobile applications. This leads an increasing demand on emerging mobile security technologies and solutions for

Manuscript received April 20, 2012; revised May 15, 2012.

The authors are with Department of Computer Science and Engg., M.A.M. College of Engineering, Anna University Tiruchirappalli, India.

mobile accesses. Hence, security becomes very important for mobile users and mobile accesses [4].The voting process in today's era is behind its time as it relates to the involvement of technology as seen by experience [5]. In countries that are more developed there are electronic voting (e-voting); these encapsulate both electronic means of casting votes and electronic means of counting votes. It can invoice transmission of ballots, and votes via telephones, private computer networks or the internet [6]. The study highlights that the full effectiveness of the smart card was not been used as the magnetic strip has the ability to store encrypted data which would use its full potential. The conclusion of that research found that significant flaws were found in that system [7]. In general, a mobile voting system has some entities which are usually used in other electronic or mobile voting systems, like in [8][9]. Although many mobile security solutions and technologies are proposed and developed in the recent years, there is lack of a comprehensive study and review about the existing mobile security issues and solutions. Whenever discussing mobile security, we must understand mobile security threats to mobile phones and mobile accesses. Mobile phones have certain specific features (such as mobility) which make these devices more vulnerable to security attacks in [10]

Biometric security is a security mechanism or technology, provided in a given application environment (or systems), identifies the individuals and their accesses of the systems by measuring their physical or behavioral attributes. There are four types of biometric-based security technologies for mobile user identification. They are: a) fingerprint recognition, b) voice identification, c) face recognition, and d) iris recognition. The fingerprint technology is the oldest one among all biometric identification. It is based on the series of three dimensional lines, called ridges, and the space between then, called valleys. The ridges and valleys are unique to a person and therefore help to verify the identity [11]. Voice-based biometric security technology identifies authentic mobile users based on their voice inputs [12]. Face recognition biometric systems are considered as the most effective security solutions for mobile users [13]. The Iris is the colored part in the eye, located behind the cornea, surrounding the pupil. Iris recognition technology is built around the uniqueness of each iris. The iris recognition based security technology in [14] provides an option of storing iris code for both irises, so that during verification, the user is required to scan both eyes. Biometric and cryptography could become complementary to each other. It is reasonable and feasible to incorporate biometric into the cryptographic infrastructure. A massive reputation has been attained for the enhanced performance of cryptographic key generated from biometrics in terms of security [15] and by abolishing the requirement for key storage using passwords, researchers in the recent past have endeavored towards merging biometrics with cryptography so as to increase overall security [16][17] [18].

III. Surrogate Object BIO-MTP System

The proposed BIO-MTP (Mobile Transaction Paradigm) system provides the reliable, fault tolerant and secured mobile transaction execution in mobile environment. Biometrics characteristics cannot be lost or forgotten and are extremely difficult to copy, share and distribute. It requires the person to be present physically. The reason behind the use of the Finger Print and Face recognition is the two persons may have the same facial structure, but it's impossible and rare that two person with same facial geometry as well as same finger print. This kind of security provides the better authentication than any other method. It also combined with the cryptography method Triple DES which is used to transmit and store the data in an encrypted format. And moreover this system contains fault tolerance mechanism, when any disruption occurs to the mobile device or to the network connectivity.

IV. Sample Application

A. Mobile Voting System

To show the usefulness of the Surrogate Object model, the following application has been developed. Consider the following application scenario: Voting by mobile devices could become a reality worldwide during next couple of years. Most of the governments are initiating this strategies and support mobile voting and in doing so, engaging more citizens in democratic process. By integrating electronic voting system with the smart phone infrastructure, the transaction process involved in this strategies become more powerful. We will consider only a single user requesting to casting his vote through his smart phone. The application can be designed using the surrogate object model in which mobile user need to query only the surrogate object for the above task if user disconnected from MSS. Surrogate object [1][2][3] is a software entity that is hosted on some mobile support station (MSS) and acts on behalf of mobile device. This helps in handling mobility of the mobile users and helps in effectively casting the vote and effectively handling of the available bandwidth for the above said application. It also acts as data cache that can collect data from database server and delivers appropriate data to the application depending upon the type of vote casting and current location of the user and its connectivity constraints. Using this model, mobile user starts communicating with the database server in a normal voting process. If the user is disconnected from the server due to energy and environmental constraints, user starts communicating with the surrogate object instead of actually communicating with database server. The application is able to exploit existing Secure Mobile authentication mechanisms and provide enhanced voter authentication and mobility while maintaining voter privacy. The following algorithm showed in fig 4, describes how this application would be developed without the surrogate object model.The Bio-MTP system architecture is shown in figure 1. In this system the user can login with their credentials via Smart Mobile device. Then the user can starts their transaction after the authentication gets successful. Next to this process, the confirmation message sends by Recovery Server, by using this message user can confirm their transaction. Once confirmed by the user the data updates into the server database. Then the successful acknowledgement

gives to the user.

B. Registration Process

The registration can be done using the mobile device by the user. During the recognition stage the following steps are performed by the authentication server. The User Name, Father's Name, Address, Voter id, Family Card Number, Password etc are retrieved from the user and these information are securely store in the vote server database. Biometric data of the voter is captured, preprocessed and features are extracted. The feature templates are formed and stored securely as enrolled templates. These saved templates are referred during the verification process. Finger print and Face sample are taken in this scheme for the purpose of final template storage in the database. The following Fig.2 depicts the Registration Process.

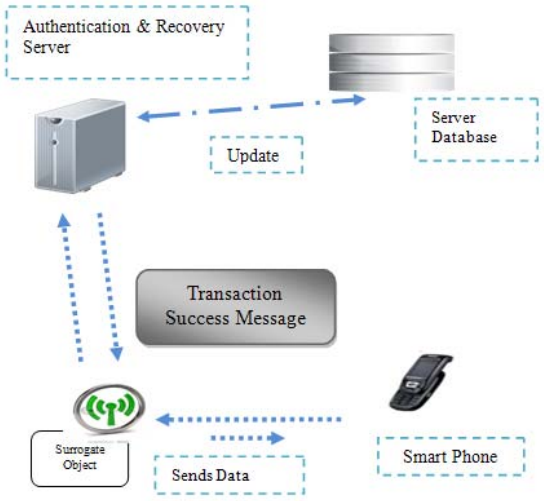

Fig.1. Bio-MTP system architecture

C. Login Process

When the voter wants to login into the server or account the authentication server, required entering their Family card number, Voter-id and Password. As shown in fig 3, the authentication server performs the following preliminary steps. Verifies the initial login credentials i.e. Family card number, Voter id and Password.

If the prior text based information is correct then the voter is redirected to the biometric authentication process and voter is asked to start camera for face recognition and provides finger print, these data are transmits through mobile device in a secure manner.

D. Verification Process

After receiving the login information and the authentication server performs the following steps.

- The server applies the reverse of the encrypted secret data procedure to recover the text information
- It verifies the received data against the text information stored in database already. If it matches the login request accepts otherwise it rejects the login request.
- If text based login credentials are accepts then the biometric data like finger print and face for the suitable voter are verified. If it matches the values in database, then authentication server accepts the user to continue, otherwise the authentication server blocks the user not to proceed further.
- Also verifies that the same user is whether already castes their vote or not. In order to satisfy the rule a person cannot cast their vote not more than once.

E. Data Transfer over the Channel

The data transfer over the unsecured channel securely is a challenge because lot of intruders and hackers may interrupt the communication and can change the information. To overcome with this difficulty, this paper proposes the use of Cryptographic method- Triple DES as shown in fig 5.

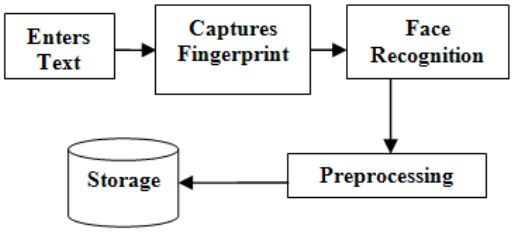

Fig. 2. Registration process

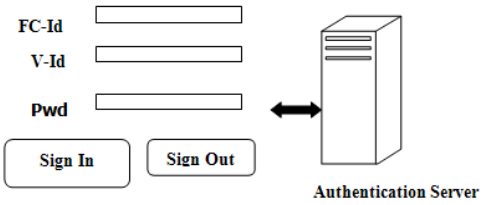

Fig. 3. Login process

The information is encrypted before the data transfer and sent over the channel using WTLS protocol. During the data transfer the time stamp is checked and it's provided that the data transfer should take place within the specified amount of time so that the chance of getting interrupted by the hackers and intruders can be reduced. The face recognition can provide for continuous authentication and can be accepted by once the user is successfully authenticated. The encryption is done using the Triple DES algorithm since it's more secure.

F. Voting Process

The authorized user can cast their vote by selecting one from the list displays. After submitting the vote there is a vote confirmation dialog box appears to confirm the selected vote by the authorized user. After the users vote gets confirmed then it stored in the database securely. Then the user suddenly gets a successful acknowledgement message from the respective server this enhances and strengthens the security and optimistic aspect of the Bio-MTP system. And then the same user cannot be vote again i.e. not more than once rule is applied to the entire user.

G. Fault Tolerance Mechanism: Surrogate Object Model

This Bio-MTP system serves a fault tolerance as shown in fig 6, when user entered the vote information the mobile device may get switch off or the network connectivity issues may occur. However the recovery server which is built in the web server that maintains complete log files to take over the failed process. And yet again it provides the service with the same entered data to the appropriate user up to where it gets

faulted. This scheme helps the user without stressing them to enter the data from the beginning. A moment the voter submits the vote. The vote confirmation dialog box appears to confirm finally to the server. Once the user confirms the vote then the cached information in the recovery server is updated into the vote server database. A disconnected operation is a regular feature in mobile computing and is distinct from failure [19]. Disconnected operation due to slumber mode is voluntary in nature and a mobile host can be required to execute a disconnection protocol before its detachment. Thus, the mechanisms have to accommodate such voluntary disconnections and make progress during the disconnection of mobile hosts. This is done by caching the current state of the Mobile Host in its place holder namely the surrogate object. However in case of disconnection due to mobility the proposed surrogate object model could help in continuing with the execution of the application using the available information cached in the surrogate object. The process involved in this strategy is explained in fig.4 and depicted in fig.6.

Normal case :

Get the Vote Request from user through his smart phone

Initialize BIO-MTP system for authentication process

If succeeds, request is forwarded to Transaction Manager at MSS.
Transaction Manager forwards the request directly to database server and performs the voting process as explained above.
Else
Vote request is rejected

Dis connection Case :

if user is disconnected
Transaction Manager (TM) forwards the request to Surrogate Object; TM checks data cache and implement BIO-MTS system for authentication at surrogate object

If Data Cache Exists
Performs the voting process as explained above
Else
request either forwarded to other surrogate objects or to other mobile devices which holds the replicas.

Fig 4. Surrogate object based voting process

V. Performance Evaluation

The Bio-MTP system provides several benefits and flexibility due to its improved security and user affable features. Some of the major benefits include; *Reduced Cost*- As the existing methods take lot of human effort and materials which is expensive. By the use of this method the cost can be greatly reduced. *Better Performance*- When compared to other existing Mobile transaction process this Bio-MTP provides better performance; the result is shown in fig 7. C*onvenience for user-Security and flexibility*- As this proposed method uses text based as well as Biometric authentication and also uses Triple DES cryptography method which provides the more security than the existing methods. The comparisons results are shown in fig 8.

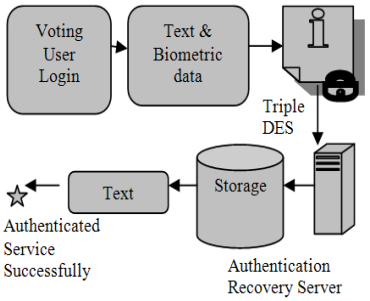

Fig 5. Data transfer

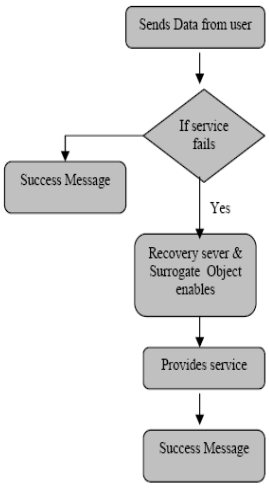

Fig. 6. Fault tolerance

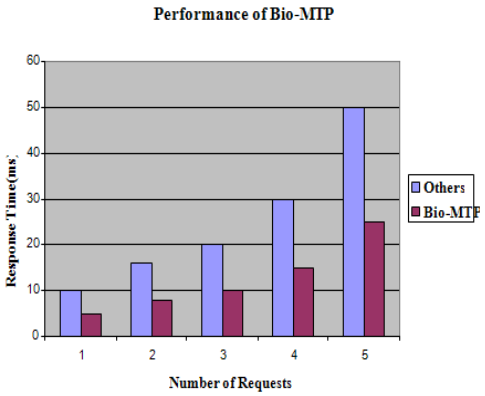

Fig.7. Performance of MTP to others

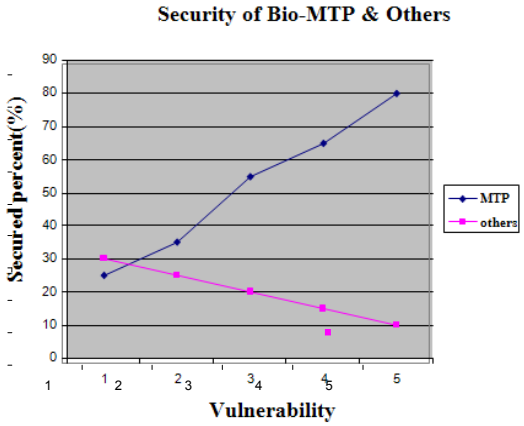

Fig. 8. Security of Bio-MTP and others

VI. Conclusion

The traditional mobile transaction system that performs the above said process can be very tedious, due to electoral fraud and cost expensive. Security is compromised because of the inability of all the human factors to provide efficient security needed for robust operation of the system. Semi-technological systems had solved some of these issues but create access to more problems because of lack of strong security. Since the general security requires Reliability, Secrecy, Integrity, Justice, dynamic, and recoverability which is provided by this proposed system Bio-MTP addressed these challenges which brings the application of text based as well as Biometric i.e. Fingerprint towards transacting from the mobile device, an additional biometric feature could be added to strengthen security such as face recognition. By using this people can perform their transaction anywhere from their mobile device. Furthermore the security features at database level should be strengthened too towards accessibility of transaction database. In addition , efficient fault tolerance mechanism which helps in case of the mobile device gets switch off or any network connectivity issues occurs, to provide an optimal mobile transaction process to an authorized user with increased reliability, which can be done by using the surrogate object model. Hence this system achieves the security goals Secrecy, Integrity and Availability with better performance which will offer a better mobile technology experience to the upcoming generation.

References

[1] M. Mohamed, M. A, J. Ram, D, and M. Chakraborty, "Surrogate Object Model: A New Paradigm for Distributed Mobile Systems," *Proceedings of the 4th International Conference on Information Systems Technology and its Applications* (ISTA'2005), May 23-25, 2005 - New Zealand, pp.124-138, 2005.

[2] S. Ravimaran, and M. Mohamed, M. A, "An Improved Kangaroo Transaction Model using Surrogate Objects for Distributed Mobile System," Proceedings of MobiDE 2011 Tenth International ACM workshop on data Engineering and for wireless and Mobile Access, June 12th 2011, Athens, Greece, 2011.

[3] S. Ravimaran, and M. Mohamed, M. A, "Surrogate Object based Data Mining for Distributed Mobile System," in *Proceedings of MoMM2011 ERPAS, ACM 9th International Conference on advances in mobile computing and multimedia*," iiWAS2011, 5-7 December, 2011,

[4] N. Jobanputra, V. Kulkarni, D. Rao, and J. Gao, San Jose State University, Emerging security technologies for mobile user access http://www.ejeta.org/issue-v2-n4/ejeta-v2-n4-2.pdf 2010.

[5] D. Gentles, Mona Inst of Appl.Sci,.Univ of West Indies, Kingston, Jamaica Sankaranarayanan, S. Biometric secured mobile voting Internet (AH-ICI), 2011 Second Asian Himalayas International Conference on Nov. 2011.

[6] Electronic Voting (2009), Available from http://www.hwskioskprinter.com/terminology_electronicvoting.pdf

[7] T Kohno et al. (2004). "Analysis of Electronic Voting," IEEE Symposium on Privacy and Security.

[8] X. Yi, P. Cerone, and Y. Zhang, "Secure Electronic Voting for Mobile Communications," in Proc. Vehicular Technology Conference, vol. 2, 2006.

[9] G. Schryen, "Security aspects of Internet voting," Proc. the 37th Annual Hawaii International Conference on System Sciences, 2004.

[10] C. R. Mulliner, "Security of smart phones," Master's thesis submitted to University of California, Santa Barbara, June, 2006.

[11] W. Jansen, R. Daniellou, and N. Cilleros, "Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation," *National Institute of Standards and Technology*, March 2006.

[12] J. A. Markowitz, "Voice Biometrics," Communications of the ACM vol. 43, pp. 66 – 73, September 2000.

[13] Y. Ijiri, M. Sakuragi and S. L. Sensing, "Security Management for Mobile Devices by Face Recognition," in *Proceedings of the 7th International Conference on Mobile Data Management*, IEEE Computer Society, 2006.

[14] S. Sanderson and J. H. Erbetta, "Authentication for Secure Environments Based on Iris Scanning Technology," IEEE Colloquium on 2 March 2000.

[15] N. Lalithamani and K. P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme," *European Journal of Scientific Research*, vol.31, no.3, pp.372-387, 2009.

[16] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," *International Federation for Information Processing 2003*, Springer-Verlag, LNCS 2828, pp. 1– 13, 2003.

[17] F. Hao, C.W. Chan, "Private Key generation from on-line handwritten signatures," Information Management & Computer Security, vol. 10, no. 2, pp. 159–164, 2002.

[18] B. Chen, and V. Chandran, "Biometric Based Cryptographic Key Generation from Faces," in *proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications*, pp. 394 - 401, December 2007.

[19] J. J. Kistler and M. Satyanarayanan, "Disconnected Operation in the Coda File System," *ACM Transactions on Computer Systems*, pp. 3–25, February 1992.

S. Ravimaran has received his **B.E. in computer science and engineering** from National Institute of Technology, Tiruchirapalli, India in 1997 and his M.E.computer science and engineering from Periyar Maniammai College of Technology, Vallam, Tanjore, Anna University, Chennai, Tamil Nadu, India in 2004.Since 2008, he has been a research scholar, pursuing a Ph.D.at Anna University, Tiruchirappalli, Tamilnadu, India. Currently he is working as a Professor and HEAD, Department of Computer Science and Engineering, M.A.M. College of Engineering, Tiruchirappalli, Tamil Nadu, India. He has published papers such as A Transaction Processing System for Sharing Mobile Databases in Wireless Environment in National Conference on Recent Trends in Information Technology at RVS College of Engineering and Technology in March 2010.Another paper titled Performance Analysis in Data Replication in Distributed Data base Environment was Published in National Conference on Networking and Database NCND organized by PABCET, on 17 -18 Mar 2005. His research interests are distributed database, mobile transaction. Professor S.Ravimaran is a member of IEEE and IEEE Computer Society, ISTE, CSI and Institution of Engineers. Mail id:ssg_ravimaran@mamce.org

G. Kanimozhi has received her B.E in Computer Science and Engineering from Shri Angalamman college of Engineering and Technology, Anna University of Technology, Chennai, Tamil Nadu, India in 2007. Since Dec 2007 to June 2010 she worked as a programmer Analyst in Cognizant Technology Solutions, Chennai, Tamilnadu, India. Currently she is pursuing M.E in computer science and Engineering, M.A.M College of Engineering, Tiruchirappalli, Tamilnadu, India. Her research interests include Networks, Network Security, and Distributed Computing. Mail id: ssg_kanimozhi@mamce.org

M. A. Maluku Mohamed has received his BE in Electronics and Communication Engineering from Bharathidhasan University, Tiruchirapalli, India. in 1993 and his M.E. in Computer Science and Engineering from National Institute of Technology Tiruchirapalli, India. in 1995.He has done his Ph.D. in Communication and Computing Paradigms for Distributed Mobile Systems in from Indian Institute of Technology Chennai, India in 2006. Dr.M.A.Maluk Mohamed was a member of ACM, IEEE and IEEE computer society, IACSIT.He was awarded Vijay Rattan by India International Friendship Society, New Delhi in 2005 for specializing in science and Technology. Mail id: ssg_malukmd@mamce.org