International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 07, July 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

MOBILE TRANSACTION CONCEPTS AND PROCESSING SYSTEM ARCHITECTURE OF TRANSACTION

Narinder Bali [1], Raghav Mehra [2]

[1] *Phd. Scholar Department of Computer Sciences, Bhagwant University. Ajmer, Rajasthan*

[2]. *Associate Professor Dep. of Computer Sciences, Bhagwant University. Ajmer, Rajasthan*

ABSTRACT

The radical evolution of computers and advancement of technology in the area of hardware (smaller size, weight, low power consumption and cost, high performance) and communications has introduced the notion of mobile computing .Mobile wireless market is increasing by leaps and bounds. The quality and speeds available in the mobile environment must match the fixed networks if the convergence of the mobile wireless and fixed communication network is to happen in the real sense. Mobile Commerce is an evolving area of e-commerce, where users can interact with service providers through a mobile and wireless network using mobile device for information retrieval and transaction processing .The challenge for mobile network lie in providing very large footprint of mobile services with high speed and security. Online transactions using mobile devices must ensure high security for user credentials and it should not be possible for misuse. Mobile computing paradigm has emerged due to advances in wireless or cellular networking technology. In this paper, we survey the fundamental research challenges particular to mobile database computing, review some of the proposed solutions and identify some of the upcoming research challenges. We discuss interesting research areas, which include mobile location data management, transaction processing and broadcast, cache management and replication and query processing. We highlight new upcoming research directions in mobile digital library, mobile data warehousing, mobile workflow and mobile web and e-commerce.

Keywords: M-Commerce, Mobile computing, Mobile database, PKI, WPKI, Wireless or cellular networking;

I. INTRODUCTION

Mobile computing provides flexibility of computing environment over physical mobility. The user of a mobile computing environment will be able to access to data, information or other logical objects from any device in any network while on the move. The First generation (1G) mobile network was developed in USA and it was using Frequency Division Multiplexing technique (FDM). A data service was then added on the telephone network which was Cellular Digital Packet data (CDPD). The network could offer data rate of 19.2 kbps. The second generation (2G) mobile network is mainly Global System for Mobile Communication (GSM) and introduced in Europe and rest of the world. The network has dedicated data channels for data transmission. The

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Third generation standards (3G) are developed by International Telecommunication Union (ITU) under International Mobile Telecommunication-2000 (IMT-2000) in order to create a global network. They are scheduled to operate in the frequency band around 2 GHz and offer data transmission rate up to 2Mbps. In Europe the ETSI (European Telecommunication Standard 206 Computer Science & Information Technology (CS & IT) Institute) has standardised UMTS (Universal Mobile Telecommunication System) as the 3GNetwork. The ITU has stated the flow expected by 4G generation should be around 1GBPS static and 100 Mbps on mobility regardless of the technology or mechanism adopted. The rapid development of mobile communication technologies and rapidly growing number of mobile devices result in fast growth of Mobile commerce. The emergence of relatively sophisticated low-power, low-cost and portable computing platforms such as laptops and personal digital assistants (PDA) have made possible for people to work from anywhere at any time (from their offices, homes and while travelling) via wireless communication network. As the technology advancing, millions of users carry portable computer and communicator devices that use a wireless connection to access worldwide global information network host should be transferred to the base station of the new cell.

II. MOBILE SYSTEM INFRASTRUCTURE

The UMTS or 3G promised advanced services such as mobile internet, multimedia messaging, video conferencing etc. UMTS standards were defined by an international consortium called 3GPP (Third generation partnership project)

2.1 Mobile computing verses distributed computing: A mobile computing system is a dynamic type of distributed system where links between nodes in the network change dynamically. A single site cannot play the role of co-ordinator as in a centralized system. The mobile host and FHs also differ in computational power and memory. The distributed algorithms for mobile environments should be structured such as that the main bulk of the communication and computation costs is borne by the static portion of the network. In a mobile environment, a DBMS also needs to be able to recover from site, network and transaction failure, as in case of distributed systems. However, the frequency of most of these failures increases and mobility complicates the recovery. In location-dependent data management, same object in different locations may have different values but still these values are considered as consistent. For example, tax object have different values in different states in United States. The most important issue remains is transaction processing in such an environment. Transaction failures may increase due to the possibility of problem during hand-off when the MU moves between cells. An MU failure creates a partitioning of the network, which in turn complicates updating and routing algorithms. Another major difference lies in the transaction model. Unlike a distributed transaction, a mobile transaction is not identified by a cell or a remote site. It is identified by the collection of cells it passes through. A distributed transaction is executed concurrently on multiple processors

III. SECURITY IN POPULAR MOBILE NETWORKS

They are: a) Entity authentication and Key agreement b) Message protection. The integrity and 3.1Security in GSM: There are two principal tasks involved for providing GSM Network security. encryption keys are agreed up on as a part of (a) and then they are used to protect messages between cell phone and base station. a) Entity

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Authentication and Key Agreement The GSM perform authentication to identify genuine users. The frequency of authentication is not specified, but the process is necessarily performed when the subscriber moves from one network to a new network.

i**. Authorization request from Cell Phone:** During authorization request step, the cell phone sends the encryption algorithm it can support to the base station and IMSI/TMSI number to the MSC. If the cell phone is away from its home network, the IMSI will be received by the MSC of the visited network. The latter communicates the IMSI to the MSC/HLR of the cell phones home network with a request to provide a challenge that will be used to authenticate by a cell phone.

ii**. Creation and transmission of authentication vectors:** The IMSI obtained by the MSC is used to index the home location registers to obtain a shared key, Ki known only to the SIM and HLR of the home network. The MSC/HLR generates 128 bit random number, RAND, which functions as a challenge in the challenge-response authentication protocol. The two quantities XRES and Kc are computed as below. XRES=A3 (RAND, Ki) Kc=A8 (RAND, Ki) Where, A3 and A8 are two keyed hash functions. XRES is the expected response in the challenge response authentication protocol. Kc is the encryption key. The HLR creates five authentication triplets, each seeded by freshly chosen random numbers. Each triplet is of the form- 208 Computer Science & Information Technology (CS & IT) The triplets are sent to the MSC of the home network by the HLR. If the cell phone is visiting a foreign network, the MSC forwards the triplets to the MSC of the visited network. Five triplets are sent so that four subsequent authentications may be performed without the need to repeatedly involve MSC/HLR of the home network. The MSC sends the challenge (RAND) from the first triplet to the base station and it is forwarded to SIM on the cell phone.

iii. **Cell Phone response**: Once the SIM has received RAND, it computes SRES (Signed Response) similar to XRES. It can be computed by an entity with the knowledge of Ki, key shared between the SIM and HLR. The cell phone sends SRES to the base station and it is forwarded to MSC. The MSC compares if SRES is equal to XRES and if they are same MSC concludes that SIM knows Ki and identifies it as a genuine subscriber.

3.1.Computation/Receipt of encryption key: The SIM computes Kc and MSC extracts Kc from its authentication triplet and communicates it to the base station. Further all communications between cell phone and base station are encrypted using Kc. Message Protection Stream cipher technique is used to encrypt the message transmission between cell phone and base station. The key stream generator for this is denoted as A5. The key stream is a function of the 64 bit encryption key, Kc, and 22 bit frame number. KEYSTREAM= A5 (Kc, FRAME_NUMBER) For each frame transmitted, the frame number is incremented which changes the key stream for each frame sent during a call. Usually cipher text is generated by X-OR ing the plain text and the key stream. Computation of the key stream and encryption do not require any static information stored in the SIM. Computation of XRES and Kc requires the subscriber authentication key, Ki. Hence the functions A3 and A8 must be supported by the SIM and A5 typically not.

IV.MOBILE COMMERCE RISKS, SECURITY AND PAYMENT METHODS

A Mobile Payment is defined as a payment for product or services between two parties for which a mobile device plays a key role in the realization of payment. In an M-Payment activity a mobile phone is used by the

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

payer in one or more steps during banking or financial transactions. The ubiquity of cell phones together with the convenience it offers suggests that mobile payments will constitute an increasing proportion of electronic payments. Mobile applications can be either be mobile web or native. Security issues in mobile web applications closely resemble those of traditional web applications because of homogeneity in underlying development technologies and protocols. There are mainly two types of mobile payments as listed below 1. Proximity Payment 2. Remote Payment In Proximity Payment, the payer and payee are located nearby and they are very close to each other. Some examples for this category of payment are the customer paying the money using their plastic cards in a Point of Sale Terminal or Customers Cell phone making a payment in a vending machine. In remote Payment, the payer and payee are located at different locations –for example they may be at different cities.

V. PAYMENT SETTLEMENT

This operation can take place during real time, prepaid or post-paid mode. A real time payment involves the exchange of some form of electronic currency, for example payment settlement directly through a bank account. In prepaid type of settlement customers pay in advance using smart cards or electronic wallets. In post pay mode the payment service provider sends billing information to the trusted third party, which sends the bills to customers, receives money back, and then sends the revenue to payment service provider.

5.1 Wireless Public Key Infrastructure (WPKI): based M-Commerce Security System Public key cryptography technique is used as backbone for the WPKI to provide security in mcommerce. The entire certificate management life cycle activities starting from certification creation, generation, storing, distribution and revocation of public key certificate is supported by an WPKI architecture.

5.2. Mobile data management: In this section, we will discuss some of the important data management issues with respect to mobile computing. Data management in mobile computing can be described as global and local data management. Global data management deals with network level issues such as location, addressing, replication, broadcasting, etc. Local data management refers to the end user level that includes energy efficient data access, management of disconnection and query processing.

5.3. Location data management: The location of mobile user is of prime importance in wireless computing. In a mobile computing, the location of a user can be regarded as a data item whose value changes with every move. In the mobile computing, the location management is a data management problem. Primary issues here are how to know the current position of the MU? Where to store the location information and who should be responsible for determining and updating of information? To locate users, distributed location databases are deployed which maintain the current location of mobile users., the hierarchical scheme allows dynamic adjustment of the user location information distribution based on mobility patterns of MUs. A unique distribution strategy is determined for each mobile terminal and location pointers are set up at selected remote locations. This reduces database access overhead for registration and there is no need for centralized co-ordination.

5.4. Data replication: The ability to replicate the data objects is essential in mobile computing to increase availability and performance. Shared data items have different synchronization constraints depending on their

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

semantics and particular use. These constraints should be enforced on an individual basis. Replicated systems need to provide support for disconnected mode, data divergence, application defined reconciliation procedures, optimistic concurrency control, etc. Ravindran and Shah [66] consider a general model for maintaining consistency of replicated data in distributed applications. It defines a casualty constraint, a partial ordering between application operations, such that data sharing is achieved by defining groups requiring it and broadcasting updates to the group.

VI. MOBILE TRANSACTION PROCESSING

A transaction in mobile environment is different than the transactions in the centralized or distributed databases in the following ways.

• As the mobile hosts move from one cell to another, the states of transaction, states of accessed data objects, and the location information also move.

• The mobile transactions might have to split their computations into sets of operations, some of which execute on mobile host while others on stationary host.

• The mobile transactions require computations and communications to be supported by stationary hosts.

• When the mobile user moves during the execution of a transaction, it continues its execution in the new cell.

• The mobile transactions are long-lived transactions due to the mobility of both the data and users, and due to the frequent disconnections.

• The mobile transactions should support and handle concurrency, recovery, disconnection and mutual consistency of the replicated data objects.

6.1 Broadcast disk and transaction processing: In traditional client-server systems, data are delivered from servers to clients on demand. This form of data is called pull-based. Another interesting trend is push-based delivery in a wireless environment. In wireless computing the stationary server machines are provided with a relative high bandwidth channel which supports broadcast delivery to all mobile clients located inside the cell. In a push-based delivery, server repetitively broadcast data to clients without specific request. Clients monitor the broadcast and retrieve data items they need as they arrive on the broadcast channel. This is very important for a wide range of applications that involve dissemination of information to a large number of clients. Pitoura and Chrysanthis addresses the problem of ensuring consistency and currency of client read-only transactions when the values are being broadcast in the presence of updates at the server.. Pitoura and Chrysanthis exploit versions to increase concurrency of client read-only transactions in the presence of updates at the servers Invalidation reports are used to ensure the currency of reads. They broadcast older versions along with new values Lee Sang-keun et al. present an optimistic concurrency control protocol with update timestamps to support transactional cache consistency in a wireless mobile computing environment using broadcast. They implement the consistency check on accessed data and the commitment protocol in a truly distributed fashion as a part of cache invalidation process with most burden of consistency check being downloaded to mobile clients. They achieve improved transaction throughput in comparison to and it minimizes wireless communication required for supporting mobile transactions.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

VII. MOBILE DATABASE RESEARCH DIRECTIONS

We see the following as upcoming mobile database research directions.

7.1 Location-dependent query processing: We present ideas for processing queries that deal with location-dependent data [51]. Such queries we refer as location-dependent. Location can be a subject of more complex aggregate queries. For example, finding the number of hotels in the area you are passing or looking for a mobile doctor closest to your present location. Hence, the location information is a frequently changing piece of data. The objective is get the right data at different locations for processing a given query. The results returned in response to such queries should satisfy the location constraints with respect to the point of query origin.

7.2 View maintenance in mobile computing: Accessing on-line database from the mobile computer may be expensive due to limited uplink bandwidth, and also due to the fact that sending messages consume lot of energy which is limited in the portable battery.

7.3 Workflows in mobile environment: Workflow management systems are growing due to their ability to improve the efficiency of an organization by streamlining and automating business processes. Workflow systems have to be integrated with mobile computing environment [4] in order to co-ordinate disconnected computing to enhance the system's resilience to failures. Specific issues that arise here include how the workflow models can co-ordinate tasks that are performed when mobile users work in disconnected mode and when they cross wireless boundaries. Also location sensitive activities might have to schedule to use an organization's resources effectively. Current workflow systems do not seem to have any provision to handle these requirements.

7.4 **Digital library services in mobile computing:** Digital libraries bring about the integration, management, and communication of gigabytes of multimedia data in distributed environment. Digital library data includes texts, figures, photographs, sound, video, films, slides, etc. Digital library system currently envisions users as being static when they access information. It is expected in the near future that users will have access to a digital library through wireless access. Provision to access digital library services through wireless networks is required by a wide range of applications from personal to research to customize business computing. Providing digital library services to users whose location is constantly changing, whose network connections are through a wireless medium, and whose computational power is low necessitates modifications to existing digital library systems. The queries in digital library are complex and involve processing, navigation, searching, and presenting of distributed heterogeneous repositories of multimedia data. There is a need to bring web on the mobile platform. Imagine a taxi that is equipped with mobile computer and the passenger there would like to browse web pages while waiting for its destination. The limited bandwidth will be a bottleneck in such a scenario. Another interesting application may be e-commerce on the mobile web. All these applications are ready to go on the disconnected, highly unreliable, limited bandwidth and unsecured platform where application demands reliability and security. Some efforts in this direction have

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

appeared in which is a WWW system designed to handle mobile users. It allows the documents to refer and react to current location of clients.

7.5 Mobile data security: Security is a prime concern in mobile databases due to nature of communication medium. New risks caused by mobility of users, portability of computers can compromise on confidentiality, integrity and availability including accountability. In a mobile database environment, it may be a good idea if data can be summarized, or only metadata can be stored on mobile platform and more detailed data can be kept on mobile service station (MSS) only. The higher frequency of disconnection also requires a more powerful recovery model. Such situations offer attackers the possibility of masquerade as either mobile host or MSS. This needs more robust authentication service . In order to achieve anonymous communication, aliases can be used or communication can be channelled through a third trusted party. Furthermore, the identity of users may also need to be kept secret from other MSSs if required. Access based control policies can be adapted to provide data security on mobile platform.

VIII. CONCLUSIONS

The widespread use of mobile devices now a day generates huge amount of revenues by reducing time and money needed for multiple purposes. The rapid development in mobile computing technology not only creates several opportunities for the business and also opens the door for doing disasters using misuse of technology. The information residing in the mobiles and integrity of the information, security of the information during its journey over the air security of the information with in the wireless network has to be given much importance. Because of Mobile Computing or Mobile networks, M-Commerce has become reality today. We have surveyed some of the problems and existing solutions in that direction. We have highlighted the merits and demerits of existing solutions. We have identified some of the upcoming research areas that require rethinking due to nature and constraints of mobile computing environment. The upcoming mobile database research directions discussed here will be the centres of attractions among mobile database researchers in years to come. There is a need to explore these issues further and improve the existing solutions offered in that direction.

REFERENCES

1. Mahmoud Elkhodr, Seyed Shahrestani and Kaled Kourouche,“ A Proposal to improve the security of mobile banking applications”, IEEE International conference on ICT and Knowledge Engineering, 2012
2. Hua Ye, “Design and Implementation of M-Commerce system applied to 3G Network platforms based on J2ME”, IEEE International conference on Electrical and Control Engineering, 2010
3. Dharma prakash agrawal and Qing An Zeng, “Introduction to Wireless and Mobile Systems”, Third Edition, Cengage Learning USA
4. Hakima Chaouchi and Maryline Laurent maknavicius, “Wireless and Mobile Network Security”, Second Edition, Wiley Publishers
5. Anurag Kumar jain and Devendra Shanbhaug, “ Addressing Security and Privacy Risks Mobile applications”, IEEE Computer society, 2012
6. Bernaard menezes, “ Network security and cryptography”, CENGAGE Learning, econd edition

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

7. ArunKumar Gangula et al., "Survey on Mobile Computing Security", IEEE Computer Society, 2013
8. Hakima Chaouchi and Maryline Laurent maknavicius, "Wireless and Mobile Network Security", Second Edition, Wiley Publishers
9. Anurag Kumar Jain and Devendra Shanbhaug, "Addressing Security and Privacy Risks Mobile applications", IEEE Computer society, 2012
10. The m-commerce architecture from "Security issues and challenges in mobile computing and m-commerce"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015
11. M payment cycle "Security issues and challenges in mobile computing and m-commerce"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015
12. Vitria Technology Inc. Available from www.vitira.com.
13. L.H. Yeo, A. Zaslavsky, Submission of transactions from mobile workstations in a cooperative multidatabase processing environment, in: Proceedings of the 14th IEEE International