Mobile database

As there was decrease in normal computing devices with consummations of the power, which lead to the concept of airless I. E. Mobile computing. This objective of this report is to check the status of mobile database and to identify research of it. In early ass's, the work for the mobile database started. Secure data transfer was the main reason introducing wireless PDA, mobile phones, etc. Which is connected to nearest mobile station and from there how the data gets transfer from remote access area in the secure manner.

This report gives you the complete outline of the participation of the mobile users in synchronization, mobile transaction, data confidentiality, and middleware adaptability. 1. Introduction There was a field in technology, were computing was the only option for some period of time. As the technologies got developed, the birth of new era with highly dynamic referred as mobile computing. This concept got developed as now a day is decrease in size of machinery and increase in computing users, which are in demand for these machinery to become part of their everyday life. Thomas Hardwood 1995) As these mobile computing technologies are evolving day by day, there are different classes of mobile applications, which can be distinguished, from the data management requirement. The common example today is the Mobile Client which acts like Fixed host where it involves traveling employees or home based employees to access the fixed corporate database from there mobile like banking data, bookmarks, weather, stock exchange, etc. (FEEL 2004) Mobile database is the database that are connected to mobile devices like smart phones, PDA over their mobile network and the database, which is carried by the mobile device.

That could be the list of contact, traveled distance, information. Mobile databases mainly concentrated in retail and logistics sector of industries. For the realization, the revolutionary concept " Mobile Computing" required wireless outwork architecture that has to support the mobile computing environment in the future distant. The basic network architecture will have the following components like Mobile Units (MO), which will be the users, then the Mobile Support Station (MS) that will maintain the communication with the users.

And there also fixed host which are connected to MS. Figure 1 : Mobile Computing Network There is also the Location Server (L'S), which maintains the data of the user location and keeps track on every mobile unit in that location. The location server's database maintains and manages the operations of the mobile wireless network. These data, which is stored in database, will be interchange among the neighboring location server and it will be used.

The mobile switching office which is corresponded by location server, will be around 70 to 100 mobile supporting stations which will be look after by one location server. We assume, each UM incorporates with a multiuse database, which are accessible by owner of UM and other users too from the remote sites (Thomas Hardwood 1995). The concept of the mobile database is a small database, which is installed, in the mobile devices. The database like Oracle, Microsoft and IBM are the major vendor for he database, which provides mobile database server.

Database provides the storage for all the communication. Agent acts like a middleware between web server and database. Web server is the link, which communicates and transfers the data between the database and mobile. Figure 2. Mobile Database Architecture (G Tornados) There are also three components on client side, Mobile database, agent and application. An agent is link of communication between the database of the mobile and database of the server and also the link between the application and mobile database. Mobile application is a GUI (Graphical User Interface), which always provide the interface to users.

The mobile database stores the replica of the same server database. The communication link should be used between the mobile database and server. Communication link HTTPS which is secure connection and several different are also there to provide the communication link like Bluetooth, 36, wireless network and GAPS (G Tornados). 4. Techniques to Secure Database The nature on how some mobile computing have introduced and work in the traditional ways. Some of the features those are required for the database, which will have the connectivity and data of all the users who is connected to it.

These areas are he traditional approach for the data management and it's system. In this report we will lists the areas for the mobile database. 4. 1 Data Synchronization: Disconnecting the work without the replication of the important data will be the issue for continuing the work. To achieve this is to replicating the data in its mobile device when it gets disconnected or by merging the data after connection is available. Disconnected the work can

also be with multi-synchronous group, where he/she will update the data which is important for the team members.

There are different tools are there which allows the synchronizing the data. Different file synchronizer (Power Merge, Microsoft briefcase, etc.), which is the non-conflicting updates which replicates the data. But still while synchronizing data conflict updates happen then? Then there are one-step further applications like Apple cloud, Microsoft Activities, etc. Allows files to synchronize the content. (FEEL 2004) The objective of data synchronization is to build synchronizer based on transformational model, which has the properties of causality, convergence and intention preservation.

The model is design in such a way that it can support disconnections for short period. 4. 2 Mobile transactions In this environment, the mobile unit generally initiates this and it is distributed among fixed units or set of devices. Mobile unit moves during their transactional execution and get disconnected partially or totally. For Mobile unit movements, procedures are requiring to support the data availability from the nearest mobile base station otherwise disconnection can happen. For this a framework has been proposed.

For transaction Mobile unit are group together for long duration transaction, which has three phases. Firstly the local environment, which has to been initialized at mobile unit in connected mode. Then the long duration transaction will be performed in disconnected mode and then it will globally committed with the local copies which are to reintegrated when mobile unit gets connection with fixed server. (FEEL 2004) 4. 3 Embedded Database

Reality and intelligent devices now a day are the pervasive computing in our every day aspects.

Now a day, when new application comes, there has been need of database techniques, which has to be embedded in various form of computing devices. There will be personal folders, data access by autonomous mobile computers and different networks, which will be the need for evaluation of queries in imputing devices. Devices like PDA, wireless phones are hand held which are the autonomous that are used to execute the on board queries. Popular Database in mobile is Sylvester that is use for Windows CE, Sybase Adaptive, Oracle ii Elite or DB Everyplace that are design for such devices.

The objective of embedded database is to have the components, which can be matched to the hardware resources that are highly constrained. Capitalizing on database work, efforts need to be undertaken. First it should show the impact on the each hardware devices on database techniques. Secondly, to have the new storage, query techniques and indexing, which will allow building the embedded database and lastly to setup the rules fro the hardware resources for the future devices that has to be match with the requirement of specific application (FEEL 2004). 4. Authentication from the Web Server As from the above architecture, the communication can be done through HTTPS between the mobile database and server database. Link is given from web server from the server side. So it is easier to take authentication at web level itself. It is important, as it provides security for the mobile database which will be executed at river end though web server. Without authentication network users wont able to connect it and it can contact the server agent for the appropriate URL. 4. 5 Data Privacy To access

the data anywhere, at anytime, anyhow has emphasizes the need of strong data security.

There has been increase in connection of the traveler users which uses their corporate database and to make their personal data available on their mobile devices have introduce threats on data privacy. Web companies' have their own privacy policies which has to accept by the mobile user has they don't have the choice. But there has been the attack on database which are frequent and these attack is normally done by any insiders. Client side security approach recently been investigated. Encryption of the data and decryption, which generally happens at client side to prevent any data loss and clear text should be shown from the server.

They have the strong servers, which provide services for backups for encrypt of the personal data. This kind of solution provides safe storage and processing the query on personal data on entrusted server. Users have to give the encryption keys if he is will to share the data and access rights too. Still sharing issues are rising. So companies are working now on the solution known as Chip Secured Data Access, which will allow the encryption of the data that will have some privileges. As all the data on embedded into that smart chip, the prevention of the tampering will not happen on client side.

This gives a guarantee against strong attack with the help of both hardware and software, which has been used in making this chip. New type of solution has been introduce to handle more complex data where embedding the users private data in his own device. But this hand held devices cannot be trusted as hey get lost, stolen and destroyed (FEEL 2004). 4. 6 Adaptability

to Middleware Users nowadays are becoming more and more practical. This involves the new context at various levels that will enable the users to gain access to their application from anywhere and at any time.

It should always have to strong software and hardware constraints. Its application should reply on the server and it should also favor the autonomous functionality and it should also be dynamic as it can fluctuates with time and place where it is. 4. 7 Communication Connection can be made through HTTPS web page. The asps code is the dynamic page, which gives the announcements. The web server should have access to read the file from database. Because of this security issue appropriate DB'S account should be there, as web server will be having access the database.

We can create d account with some permission where our data cannot be written again and will always be ready only to other users who are accessing it. 4. 8 Data Encryption at Client Side We have to test all the features for encrypting the data in the database. It is considered as an important feature for securing the database of the mobile and its application. The user has to give the password to the application and his private and priority data will store permanently in the database. This kind of encryption guarantees the data confidentiality against any user in the database. 5.

Resisting the Attacks Ensuring and giving proper security to the following things can achieve the security: * For Mobile device * For server * For communication link * For application We have to test the tolerance of the security against any threats or attack. Threats can be from user, which has the access to communication link, and from read only user. Attack on Mobile

devices: As the mobile database is encrypted to ensure confidentiality of the data if mobile devices gets attacked or stolen. If the mobile is attacked through network when synchronization when it is connected to the network.

When it is connected to network for the short period it can be targeted by malicious software as mobile does not have the build in firewall where it can protect. And the data, which is stored in mobile database, are normally encrypted and will not bale to read any content. If the device gets stolen: If the mobile gets stolen, the data in that vice is encrypted so the data is not readable. Attack on Server: the access the server data, it should the right and permits to access the network when an incoming connection is made with the web server.

We can apply some techniques so as to protect the server. 6. Conclusion In this report, we have reviewed the progress of the mobile database. To develop the mobile database which has to be secure will be an important task. There as been effort to implement an application on the mobile database which will be reliable, reasonable and efficient. Fro the security concern, this report has given the quinine to secure the data and they all are sufficient tools to provide the appropriate security level.

We have also identifies the techniques like synchronization, privacy, database embedding, adaptability to middleware, authentication and connection between server and client side. Improvement in the existing solution, we would like more general and simple solution where it should have the proper model of interface and languages for validations in real time mobile settings. The communication will intermit. Database will be set up

and coping up with the same on road networks, and to cope up with uncertain conditions like while revealing and environmental condition.