Abstract

Devices such as smart phones are considered to be the most common communication devices in current scenario. Recently, mobile phones are not only used for voice and message communication but also, sending and receiving important data such as social security numbers, bank account details and passwords, so it is important to provide proper security to the data's in the distributed mobile environment. Although there is lots of security
mechanisms have been proposed already, a lot more needs to be done. We have proposed a new security model that prevents data leakage among object based transaction execution in distributed mobile environment. The model first secures the data on the object by authenticating the user and then secures the data during transaction execution and reconciliation. The proposed mechanism is efficient in securing the data because communication has been reduced by making the object to act on behalf of the server. It also ensures confidentiality of transaction by creating an encrypted tunnel between the objects and database server. The entire process is simulated and results shows that our model is more secured and provide less communication overhead than the existing models in the distributed mobile environment.

References

- X. Ding, D Mazzochi, and G Tsudiatures&quot;, ACM Transactions on Internet Technology (TOIT), 2007.
- Fangguo Zhang, Yi Mu, and Willy Susilo, &quot;Reducing Security Overhead for Mobk, &quot;Equipping Smart Devices with Public Key Signile Networks,&quot; The proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA&amp;apos;05), Vol. 1, 2005.
- M. A. Maluk Mohamed, D. Janakiram and Mohit Chakraborty &quot;Surrogate Object Model: A New Paradigm for Distributed Mobile Systems&quot;.
- Millan, W. , Gauravaram, P. , 2004. Improved Attack on the Cellular Authentication and

Index Terms
Computer Science
Hpc Applications

Keywords
Security Authentication Surrogate Object Confidentiality.