Survey paper on banking system using location-based system

Finance, Banking

Abstract - Increasing digitaltechnologyhas revolutionized the life of people. The banking system in today’s world is open to threats of fraud and cyber-attacks. Since today's banking system is built on location-based, it is easy for an attacker to penetrate in any such database which will easily compromise all the information and data of the customers of the bank.

This vulnerability of today’s banking system can be reduced by re-building the banking systems on top of location-based technology, thus reducing the threat of the database being hacked. Since the user is accessing an account within a particular geographical location then the only user can access or transfermoneyotherwise not it will make the transactions more secure thus making the overall banking system faster and secure.

Index Terms - location based, Banking system, AES

INTRODUCTION

Smart phones are becoming a major part in everybody’s daily life. All kinds of activities, including banking or financial mCommerce transactions (e. g. online shopping), are nowadays performed online via Smartphone applications whilst on the move. 50% of all Smartphone owners in the U. S. used their Smartphone for banking transactions in the first quarter of 2011. This is an increase of nearly 100% compared to the year before [1].

However, most of the techniques used to authenticate the client towards the remote authenticator (i. e. the bank offering a financial service) in these mCommerce applications still base upon classic (and static) authentication factors like passwords, tokens or biometrics.

The fact that the client is on the move, whilst using these mCommerce applications is not considered or used to enhance the authentication security. Reliable client authentication and data protection are still major concerns for mCommerce application providers because the classical authentication factors are open for hackers.

As a result, mCommerce application providers restrict access, on average, to 30% of possible services to their clients via Smartphone applications. Financial institutions engaging in any form of Internet banking using smart phones should have effective and reliable methods to authenticate customers.

An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet bankingenvironmentcan result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. This paper presents a solution to implement a Secure Authentication mechanism which is based on an active securing Fund Transaction and securing login credential using Location Based Authentication.

RELATED WORK

In this Paper, This paper proposes a location-aware attribute-based access control scheme for cloud storage, in which the location information is flexibly set as trapdoors inside fundamental access policies of CP-ABE, and trapdoors are released with the help of location servers. The trapdoor approach makes that the change of users' locations will not cause revocation of users' attributes.

Our analysis shows that the above approach is effective and our proposed LABAC brings little overhead to data consumers, attribute authorities and the cloud.[1]

In this paper, we have covered several novel technologies that use mobile devices to access different services from anywhere and anytime. The definitions, the advantages and the architecture of each technology is explored. The mobile cloud computing technology was taken, recently, more consideration a caused to its importance.

Because mobile devices in continuous and quick development, they are taken a care from IT developers. Mobile cloud computing will be the dominate technology and the trend now is to develop new applications and to remodify the old applications to be mobile cloudy. We tried to prove that this technology will conquer the challenges and the problems of preceding technologies. Mobile cloud computing models are presented.

These models try to alleviate the problems concerning the limited resources in mobile devices. Despite the enormous development of mobile devices and

the support of mobile cloud computing to mobile devices, they still take a lot of attention of researcher because a number of challenges encounter this technology. We are interested to work in this domain and, for future research, we will concentrate on its challenges and explore it deeply.[2]

In this paper, we have undertaken a systematic literature review of mobile cloud computing (MCC), in order to understand the trend of research interests so far in MCC, in terms of the least and most researched issues. We were able to highlight some of the challenges in MCC such as privacy, security and trust, fault tolerance, mobility management, network congestion, heterogeneity and connection protocols, resource constraint and platform heterogeneity, context awareness, presentation and usability issues, battery life and energy awareness, and cloud API Security Management.[3]

In this paper, we tend to propose a unique authentication theme for mobile cloud computing, Data Digest-based Authentication consists of 3 phases: registration, authentication, and update. With these phases, Data Digest Authentication utilizes hashing, additionally to traditional user id and secret primarily based authentication, to make sure confidentiality and integrity throughout the authentication method. It can survive a range of various attacks, like man-in-the-middle, replay attacks, etc.[4]

Cloud computing is the present and futuristic resource pooling paradigm which converges with the Internet of Things (IoT). However, there are authentication and key management issues to be resolved. Identifying users

is not an easy task in cloud. As a result in this article we proposed a provably secure multi-factors authentication scheme with trusted third party. In our approach, trustee distributes the authentication tokens on behalf of cloud service provid¬ers and allows the cloud servers just to verify the hashed key credential data.

This approach also ensures the mutual authentication of thecommunicationentities. We used multi-party station to station Diffie-Hellman key exchange protocol which overcomes many key management prob-lems. Our proposed mechanism preserves the privacy of the remote authentication details in the cloud and significantly helps to protect the stakeholder’s sensitive information from the inside and outside malicious attackers.[5]

EXISTING SYSTEM

In the existing system several challenges, including security and privacy are raised from the adoption of this IT paradigm. A major challenge in cloud and mobile cloud computing is to ensure security and privacy of users personal information (e. g., financial data, healthrecord, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients.

PROPOSED SYSTEM

In this paper, The proposed authentication scheme provides a true protection for the user credentials in the cloud. Therefore the problems and risks envisioned in the previous section can be achieved. Advanced Encryption

Standard (AES) algorithm is used for symmetric encryption/decryption of communication data between users and servers.

A major challenge in cloud and mobile cloud computing is to ensure security and privacy of users personal information (e. g., financial data, health record, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients. Authentication is important for establishingaccountabilityand authorization of the users while allocating cloud resources.

These days, mobile devices are built with features that allow them to access the clouds resources. The devices are made to easily access the resources due to their portability and ease of use. This architecture is the same as the client server architecture. The second purpose of the mobile device is to act the node for the cloud where resources are gathered from all the mobile devices that are participating to solve the problem of processing power and limited storage. The methodology of the system is:

1. User: The data consumer (User) is assigned a global user identity Uid. In the proposed system the user send request to the cloud server for accessing the information (transaction).
2. Admin: Admin can add user and monitors system.
3. Cloud: In cloud we can stored and access data.

4. Location-based Authentication: In this module If user is accessing a account within particular geographical location then only user can access or transfer money otherwise not.

CONCLUSION AND FUTURE WORK

In this system we proposed a novel fully secure location-based mechanism based on a Advanced Encryption Standard (AES) scheme. To protect user's confidential information, data should be accessible by the authenticated people only. To achieve this aim, location based authentication methods are used.

REFERENCES

1. Yingjie Xue, Jianan Hong, A Location-aware Attribute-based Access Control Scheme for Cloud Storage.
2. Erlangung des doktorgrades, Biometric cryptosystems: authentication, encryption and signature for biometric identities.
3. Ahmed Dheyaa Basha, Mobile Applications as Cloud Computing: Implementation and Challenge.
4. Prof. Mamta sharma, Study on mobile cloud computing, it's architecture, challenges and various trends.
5. Zhangjie Fu, Xingming Sun Towards Efficient Content-aware Search over Encrypted Outsourced Data in Cloud.
6. Y. Zhu, D. Ma, D. Huang, and C. Hu, " Enabling secure locationbased services in mobile cloud computing," in Proceedings of the 2nd ACM SIGCOMM workshop on Mobile cloud computing. ACM, 2013, pp. 27–32.

7. J. Shao, R. Lu, and X. Lin, " FINE: A ? ne-grained privacypreserving location-based service framework for mobile devices," in Proceedings of the 33rd IEEE International Conference on Computer Communications. IEEE, 2014, pp. 244–252.
8. S. Yu, C. Wang, K. Ren, and W. Lou, " Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010, pp. 261–270.
9. K. Yang, X. Jia, and K. Ren, " Attribute-based ? ne-grained access control with ef? cient revocation in cloud storage systems," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 2013, pp. 523–528.
10. D. Boneh and M. Franklin, " Identity-based encryption from the weil pairing," in Proceedings of the 21st Annual International Cryptology Conference. Springer, 2001, pp. 213–229