ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Sedas for Securing E-Banking with LBA using smart phone

Dhore Mayuri Bhaskar[1]
Dept of Computer Engg
Dr. D.Y.Patil IET
Ambi, Pune – India

Pagade Amruta Vasant[2]
Dept of Computer Engg
Dr. D.Y.Patil IET
Ambi, Pune – India

Mhalaskar Vidya Sudhir[3]
Dept of Computer Engg
Dr. D.Y.Patil IET
Ambi, Pune – India

Gaikwad Swapnali Mahadeo[4]
Dept of Computer Engg
Dr. D.Y.Patil IET
Ambi, Pune – India

Abstract: ***In this paper, we propose a location based authentication and authorization scheme for mobile transactions using smart phones. Location-based authentication is a new direction in development of authentication techniques. Authentication and authorization are two of the most important security features for mobile transaction systems. We Uses space Time Authentication Technique that uses GPS system for a position determination of the person. Most commonly, these schemes depend on three factors: what you know (secret), what you have (token), and what you are (biometrics). Here, we use SeDas System with the basis of Shamir's Algorithm for Secure Fund Transaction. This paper first describes the architecture of our proposed solution, protocol including three parts: location registration, authentication and authorization and location verification etc.***

Keywords: location; authentication; authorization; mobile; data privacy, self-destructing data; system GPS; AAA.

I. 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's. 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. 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. This paper reviews techniques that use location as an authentication factor, and makes recommendations how location can be used to enhance the security of banking using smart phone applications requiring robust client authentication and lastly how secret key using shamirs algorithm will ensure securing fund transaction. Authentication is one of the three main processes of AAA systems (Authentication Authorization Accounting).

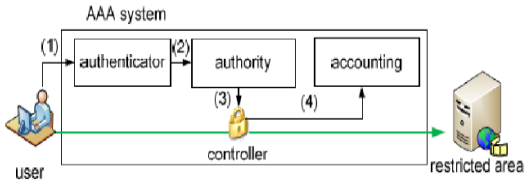

Figure. 1 Generic System AAA

When a user wants to get access to the restricted area, he has to be authenticated by authenticator (1). It depends on user's identity authority whether grant or not the access to the restricted area (2). If the access is granted, controller establishes connection between the user and the restricted area (3). Accounting records information related to user's actions (4) is created. Authentication techniques are commonly classified into three main groups as:

1. User has something – techniques using RFID (Radio Frequency Identification Device), hardware keys, etc.;
2. User knows something – this group is based on knowledge of confidential information, for example password authentication;
3. User is someone – biometric techniques that are limited to a human authentication.

Location-based authentication can be useful in many cases. The advantages of location-based authentication present the first place of usage can be found in the hospital sector. A doctor shouldn't handle with patients' privacy information out of hospital's border. Another example of location-based authentication we can find in the financial branch. If a user (account owner) would like to operate on his account, it should prove his location at first. If the user is at home or in the bank office, he will get the access. If he is on another position, he won't get the access to his bank account. In general, location-based authentication techniques can be used also for SSO (Single Sign On), but techniques proposed in this paper principally assume simply authentication (one identity per user).a self-destructing data system, or *SeDas*, which is based on an active securing Fund Transaction and securing login credential using Location Based Authentication. The SeDas system defines a self-destruct method object that is associated with each secret key part and survival time parameter for each secret key part. In this case, SeDas can meet the requirements of self-destructing data with controllable survival time while users can use this system for managing secure fund transaction over the internet.

II. System Objectives

Project scope is the part of project planning that involves determining and documenting a list of specific project goals, deliverables, tasks, costs and deadlines. We have defined a broader scope for the project as follows;

1. To design a Front Application for Android Smart Phone through which the user can interact with the system for performing Banking Transaction.
2. To design a Banking Server Architecture where communication messages will be stored.
3. To define a Self Destruction (SeDAS) scheme to provide strong security for fund transfer using key self destruction mechanism based on time.
4. Login Credential using User geographical Locations.
5. GPS Interface

III. Literature survey

A. SEDAS: A self-destructing data system based on active storage framework

This paper proposes a distributed object-based storage system with self-destructing data function. We use SeDas system with the help of Shamir's algorithm for secure fund transaction. This system combines a proactive approach in the object storage techniques and method object, using data processing capabilities of OSD to achieve data self-destruction. User can specify the key survival time of distribution key and use the settings of expanded interface to export the life cycle of a key, allowing the user to control the subjective life-cycle of private data. Vanish is a system for creating messages that automatically self-destruct after a period of time. The key is permanently lost, and the encrypted data is permanently unreadable after data expiration. Vanish is an interesting approach to an important privacy problem, but, in its current form, it is insecure. Vanish is the previous approach of the Sedas System, it also based on key generation algorithm but at a time it generate only one key so instead of that Sedas generate multiple keys with the help of shamirs algorithm so its better for security purpose. Also, we presented an improved approach against *sniffing attacks* by way of using the public key cryptosystem to prevent from sniffing operations.

B. Location-Based Authentication and Authorization

A fair number of research studies have been performed in the area of location-based authentication and authorization so author of the previous paper high light its importance for improving network security. In previous paper the concept of LBA is not secure, so in this paper we improve this concept. We uses location for the security purpose, so if in any case the ID and password may get hacked but still because of location the security is maintain. No one can guess the location that has been provided by user. User also can change the location as per their need. In addition, the previous approaches require extensive user involvement making them less user–friendly. With the current technology it is possible to make this technology transparent and convenient for users and it is also user friendly.

IV. DESIGN AND IMPLEMENTATION

Our proposed solution comprises six components, which are combination of various servers and applications:

I) **Location-based ID (LBID) server** – is the core component of our solution, which stores users' location information and authorization policies. It provides location registration, authentication and authorization services;

II) **Certificate Authority (CA) server** - provides certification of all system participants, issuing, managing and distributing their certificates;

III) **Authentication server** - provides authentication service for all participants. It can be any existing authentication service, such as username-password authentication. And it is extended to connect with the LBID server to provide location-based authentication service;

IV) **Authorization server** - provides authorization services for all participants. It can be any existing authorization service, such as role-based authorization. And it is extended to connect with the LBID server to provide location-based authorization service;

V) **Service Provider (SP) server** - provides various mobile services; and

VI) **Location-based Client (LBC) Application** - an application running on user's mobile device, capable to collect location information from trusted Location Providers (LP) and providing user interfaces to register, store and manage location data.

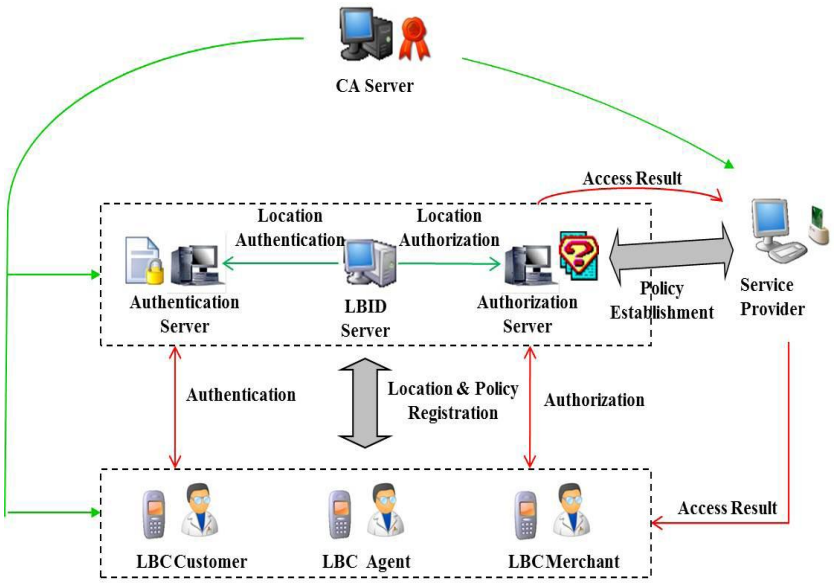

Figure 2 Location-based authentication and authorization architecture

The architecture and components are shown in Figure 2. System setup is performed by system administrators, establishing location-based authorization policies and certifying all system components. Users then use LBC to interact with

LBID server and Authorization server. After valid and successful registration of their current location, users submit access request to Authentication server, which interacts with LBID server and Authorization server to evaluate the request based on the information registered in LBID server and on authorization policies registered in the Authorization server. The result is sent to the targeted SP server, which decides accordingly to either allow or deny access request. One of the most important concerns of location-based services is security and privacy of the location information. In order to protect location information and the privacy of user's location, we use cryptographic techniques, based on Public Key Infrastructure (PKI) and certificate mechanisms. The details of certification issuance and distribution in a mobile environment are not described in this paper. It is assumed that every entity has already received certificate. All certificates are issued by CA server in a standard way. In that way, the integrity of location data sent from LBC to LBID server can be verified. All the messages exchanged between all components are digitally signed by message initiator.

V. ALGORITHM

Shamirs algorithm

- In cryptography, **secret sharing** refers to a method for distributing a *secret* amongst a group of participants (in our case it is Account Holder and Bank Authorized Member), each of which is allocated a *share* of the secret.
- The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.
- Goal is to divide some data *D* (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that:
- Knowledge of any k or more D pieces makes D easily computable.
- Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is called (k,n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.
- Suppose we want to use (k,n) threshold scheme to share our secret S where k < n.
- Choose at random (k-1) coefficients a1,a2,a3…ak-1 , and let S be the a0

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1}^{k-1}$$

- Construct n points (i,f(i)) where i=1,2…..n
- Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

VI. CONCLUSION

In this paper a location-based authentication and authorization mechanism using smart phones is proposed and described. The proposed solution provides comprehensive protections for transmission, procession and verification of location information. For location verification, we propose a hybrid approach, which combines various technologies. This approach improves the confidence of verification results, compared with other solutions where only one factor is used for location verification. As a result, our location-based authentication and authorization mechanism becomes more secure and valid. The use of location however is just the first step in using contextual information for improving security mechanism. As the Smartphone technology progresses more and more sensors are integrated into the devices e.g. Proximity sensors, near field communication (NFC) and

so on. This offers even further opportunities to capture and include this information about the user's environment on top of his/her location.

References

1. A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
2. Denning, D. and Macdoran, P., "Location-based Authentication: Grounding Cyberspace for better Security", Computer Fraud & Security, 1996(2), pp.12-16.
3. Jansen, W. & Korolev, V., "A Location-Based Mechanism for Mobile Device Security", in WRI World Congress on Computer Science and Information Engineering, Los Angeles, California USA, pp. 99-104, 2009
4. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proc. USENIX Security Symp., Montreal, Canada, Aug. 2009, pp. 299–315.
5. YounSun Gho, L. Bao, M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol", Mobiquitous, Third Annual International Conference on Mobile and Ubiquitous Systems, Networking, and Services, pp.1-7, 2006

