Article can be accessed online at http://www.publishingindia.com

# Implementation of Location Based Authentication for a Remote Client

**Laxmi Arun[*], Mahima M. S.[**], Rashmi R.[***], Roshini Prasad G.[***], Sachin Jain S.[***]**

**Abstract**

Mobile networks provide distinct set of services for the user in which authentication is one of the imperative and significant types of services. There are various factors of authentication. Some of them are passwords, security token, retinal scan, fingerprint, and other bio-metric data, etc. The other new factor is the user's location which can also be used as one of the criteria for remote client authentication. However, the information of location is private and can be misused; hence distinct procedures should be implemented to ensure its integrity.

In this paper, we propose the use of location based services to provide authentication to a remote client. As a use case, we consider the Automated Teller Machine (ATM), which is one of the most popular targets of fraud today. A remote client is provided with necessary authentication using the location based services, defined by the Expand LRAP (Location based Remote client Authentication Protocol), so as to make him aware of a genuine ATM where he can carry out secure transactions.

**Keywords:** Location Based Remote Client Authentication Protocol, Authentication, Global Positioning System, Remote Client Authentication, Advanced Encryption Algorithm, One Time Code

## 1. Introduction

Authentication is defined as the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or a software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification.

Authentication is one of the vital procedures because data may be confidential, thereafter integral methods to ensure that they are protected are in the interest of the scenario. Several methods are deployed for this purpose, yet they are subjected to attacks and intrusions.

There are three factors/types of authentication - one-factor, two-factor and three-factor:

The first type of authentication is something that the user claims to know. The most recognized form of one-factor authentication is the traditional static password.

The second type of authentication is in addition to the first factor-something that the user has-which could be an ID card, security token, mobile device or cell phone.

The third type of authentication is something that a user is, in addition to the previous two factors. Examples of third factor authentication include fingerprint, retinal scan, voice recognition pattern or other biometric data.

In this paper we propose LRAP (Location-Based Remote Client Authentication Protocol) which combines several authentication factors such as passwords and one time tokens combined with the use of a physical device that a person owns, such as a client card or a mobile computing device to securely authenticate a mobile user.

* Assistant Professor, Department of Computer Science, Vidyavardhaka College of Engineering, Mysore, Karnataka, India.
** Department of Computer Science, Vidyavardhaka College of Engineering, Mysore, Karnataka, India
E-mail: mahima.6.ms@gmail.com
*** Department of Computer Science, Vidyavardhaka College of Engineering, Mysore, Karnataka, India.

## 2. Organization

The paper is organized as follows: in Section III we present the related work, in Section IV we present a use case used as a starting point for our work, in Section V we describe our proposed location-based remote authentication protocol, and in Section VI we provide solution for the presented use case using LRAP. Finally, in section VII we conclude our paper.

## 3. Related Work

### 3.1. Location Authentication

Location authentication assures the truthfulness of the claimed or presumed location information.

It is a means of providing a higher level of security using location as a major authentication factor, along with other factors like user-id and passwords. The location-based authentication is gaining importance because of the increased use of mobile devices.

### 3.2. Location Authentication Problem and Some Solutions

The U.S. space-based Global Positioning System (GPS) is used as a source to obtain the location information. For anyone with a GPS receiver, the system provides accurate location and time information in all weather, day and night, anywhere in the world. However, from the security point of view, the authenticity of the GPS signal is not guaranteed because, a false (or spoofed) GPS signal could be generated by a dedicated GPS signal simulator, and a typical GPS receiver would not be able to detect that.

Some "advanced" GPS receivers are enhanced with anti-spoofing modules in order to detect whether the GPS signal comes from the satellite or from a fake GPS simulator. In the recent years, more and more advanced GPS simulators are being designed which makes it difficult *delete this and insert* "to identify whether a signal comes from a "real" source or not. In order to cope up with this problem, many software methods are being made available, which use the intermediary measurements directly available in the GPS receivers to detect spoofed signals and also enable recovery of the authentic signals in some cases.".

## 4. ATM as a Use Case

An Automated Teller Machine (ATM) is a computerized machine that provides the customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions, without the need of actually visiting a bank branch.

ATMs are the one of the common targets of fraud. Fraud against ATMs and people's attempts to use them takes several forms.

### 4.1. Common ATM Theft Scams

Some of the common ATM theft scams are as follows:

1. **The Lebanese Loop**

Many thieves are using external devices to confiscate the client card. The Lebanese Loop refers to a kind of ATM fraud where a blocking device (which can be as simple as some film glued to trap ATM cards), is inserted into the card slot of the ATM "machine" needs to be omitted. This card is retained by the machine because of the presence of a strip or sleeve of metal or plastic within the machine, and is retrieved by the fraudster when the card holder leaves.

2. **Card Skimming**

Card skimming refers to the illegal copying of information from the magnetic strip of a credit card or ATM card. It is a more direct version of a phishing scam. Skimming devices are often mounted beside a normal ATM card slot with a sign that says, "Slide card here first". Once scammers have skimmed your card, they can create a 'fake' or 'cloned' card with your details on it. The scammer is then able to run up charges on your account or even commit an identity fraud.

3. **Shoulder Surfing, Fake PIN Pads, and Even Fake Machines**

Thieves may mount a wireless video camera inside the ATM area. In this way, the thieves may obtain the PIN number and use it to make magnetic strips and hence reproduce fake ATM cards.

Fake PIN pads may also be placed on top of the original ATM PIN pad. Unfortunately, with such fake PIN pads,

ATM transaction will proceed normally and the user won't know that his PIN information has been stolen until it's too late.

Thieves have also taken to putting up fake ATMs in and around shopping centers and other public locations. Placing the client card into the card reader, will enable the machine to collect the ATM PIN and account information. These machines do not dispense cash. Rather, a transaction failure message such as "Machine is out of money" or "Machine is out of order" is displayed on the display screen.

**4. Cash Trapping.**

Similar to the problem of Lebanese Loop, a blocking device is placed on the cash dispenser which collects all the money. The transaction will take place normally but the user will not be able to withdraw the cash.

In such a case the client may walk away thinking the machine is defective or may register a complaint at the bank. The ATM switches off after reporting an error. Either way, when the user leaves the ATM, thieves can walk up; remove the device and the cash.

In our work, we address the first three ATM scams mentioned above.

## 5. Location based Remote Client Authentication Protocol

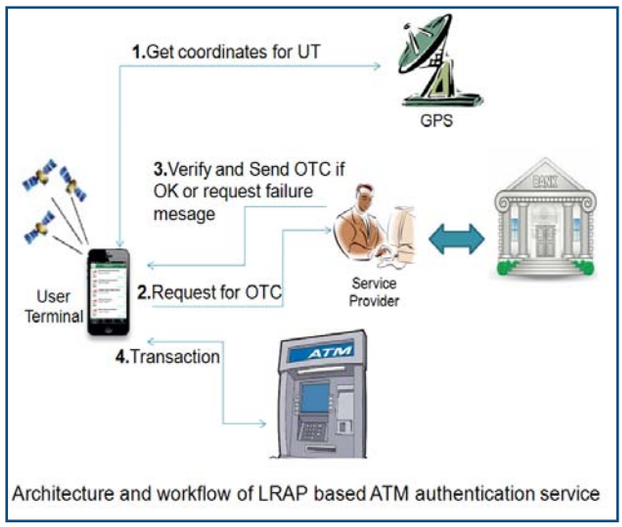
LRAP is based on three authentication factors: where a person is and when – i.e. the location of the user associated with the time information, something suppose, an application the user has - a GPS aware terminal, a piece of information the user recognizes, that is a static PIN (Personal Identity Number) adopted to access the device and an OTC.

LRAP architecture involves several actors, i.e. the user and the User Terminal (UT), the Service Provider (SP) and the Global Positioning System (GPS). The basic architecture of an LRAP based ATM authentication system is shown in figure 1.

### 5.1. User and the User Terminal (UT)

A user holding a bank account is given a privilege of a mobile application .He creates an account in it with the registration of his user-name and his respective IMEI (International Mobile Equipment Identity), which is unique for every mobile.

**Figure 1**




Architecture and workflow of LRAP based ATM authentication service

As part of the registration, the user provides several data to the Service Provider (SP), such as: (1) person identification data, like name, surname, birthplace; (2) UT identification data, such as the phone number and the IMEI (International Mobile Equipment Identity) code uniquely identifying the UT device in the cellular network; (3) other data, such as a bank account number (if a payment operation need to be performed in the service), or service subscription type (silver, gold).

The time when the need of a transaction arises, the user approaches an ATM and opens up the application in his mobile, to send a request for an OTC (One-Time Code) to the server. The moment the application opens, (comma missing) the user's location is also being processed and hence seen through. Then the location of the user, IMEI and the request for the OTC is sent to the server.

### 5.2. Service Provider (SP) and the Server

A Service Provider (SP) maintains a database containing the list of all the ATMs, their respective locations and the banks that have set up the ATMs. The server also contains a list of authorized customers of a bank who have obtained ATM cards.

When the server obtains a request for an OTC from a user, the SP verifies whether a genuine ATM is present

at the obtained user's location. If yes, the SP then checks whether the obtained IMEI is in the list of the registered customers, otherwise a message is sent to the user saying the ATM is not genuine at the given location. Next, if the IMEI verification succeeds, the server generates an OTC and sends it to the user. The user can make his transactions using this OTC.

### 5.3. Global Positioning System

We include the LocationManager class to get the respective user's location. This class provides access to the system location services. These services allow applications to obtain periodic updates of the device's geographical location, or to fire an application-specified Intent when the device enters the proximity of a given geographical location.

If the location is not accurate then a manual button is given as an option where in the user is shown in a particular radius. Then the user inputs the exact location.

When the user requests for the OTC the current location is sent to the server along with IMEI number.

### 5.4. Concept of OTC

A traditional, static password is usually only changed when necessary: either when it has expired or when the user has forgotten it and needs to reset it. Such passwords are cached on computer hard drives and stored on servers and are hence susceptible to cracking.

A one-time code (OTC) is a password that is valid for only one login session or transaction. In case of one-time codes, even if an intruder manages to record it, he won't be able to abuse it, since it will be no longer valid after being used once.

Most of the OTC generation algorithms make use of pseudo-randomness or randomness. This is necessary because otherwise, it would be easy to predict the future OTCs by observing the previous ones.

### 5.5. Advanced Encryption Standard

Advanced Encryption Standard (AES) is a symmetric-key encryption algorithm, meaning the same key is used for both encrypting and decrypting the data.

AES is used as part of providing authentication for the communication that takes place between the UT and the SP. The Service Provider generates an encrypted OTC at the Server side. This encrypted OTC is received at the User Terminal and decrypted so that the user can understand, to be able to use the generated OTC. The user can then carry out his transactions.

## 6. Providing Solution Using LRAP

1. **The Lebanese Loop Problem**

Even if the thieves get the ATM card as well as the PIN number from the victim, they will not be able to access the user's account unless the OTC (which is used as the PIN number) is generated.

OTC is generated by the service provider only when the user requests for the OTC using his/her mobile application, since it requires the user's mobile's IMEI number. The thieves do not have access to generate the OTC and hence cannot use the ATM card anywhere across the globe to access the account. Meanwhile, the user who has lost the ATM card can provide information to the bank saying that the ATM card has been lost and cancel all the transactions that might take place via that ATM card.

2. **Skimming Devices**

The skimming devices that are added to the ATMs by the thieves obtain the user's account number, password, etc. Later the thieves may create fake cards using the obtained information and use them either to perform transactions in the future or sell the fake card with the password to others. Even if such cards are created, since every time a new, one-time use password i.e. OTC is to be used, the thieves cannot perform the transactions using the same old password that was once retrieved by the skimming device.

3. **Shoulder Surfing and Fake ATM**

Shoulder surfing and fake PIN pads problem can be overcome in a similar way as explained in the skimming device problem. Suppose if fake ATMs are put up, still the user makes use of his/her mobile application to obtain the OTC for transaction from the service provider. The service provider before sending the OTC to authenticated user, first checks whether an ATM is present at the location obtained from the GPS co-ordinates of the user terminal

in the server database. If a fake ATM machine is placed then the user will not obtain any OTC from the service provider, instead a failure notice is received saying the machine is not genuine.

## 7. Conclusion

Authentication plays a major role in ensuring security. There are three types of authentication i.e., one factor, two factor and three factor authentication techniques. In our work, we propose Location based Remote client Authentication Protocol to provide authentication for a remote user, considering location as the factor. There are distinct approaches on how the location is calculated and put into use, and we have briefed about the GPS which obtains the location factor.

We have considered the ATM as a possible use case and have proposed the implementation of LRAP which will allow a client to perform secure transactions at the ATMs, especially in remote places. ATM scams and frauds such as the Lebanese Loop, Card Skimming, Fake Machines and Cash Trapping are very popular and are increasing every day. To avoid these issues our prospective can be looked upon.

The user runs an application which obtains his/her location and sends a request for a one time code (OTC) to the Server. The request is acknowledged and an encrypted OTC is sent to the user using which he/she performs a safe transaction.

Our work does not deal with all the issues and there is a room for future enhancements which may be to overcome cash trapping in ATM. An offender may insert a cash dispenser in a genuine ATM and the amount of the transaction unjustifiably drops into it. A solution to avoid cash trapping is not yet devised, but a user is expected to be aware of the ATM architecture and look out for possible frauds.

## References


1. Schneier, B. (2005). Two-factor authentication: Too little, too late. *Communications of ACM*, April, 48(4), 136.
2. Berbecaru, D. (2011). *LRAP: A Location-Based Remote Client Authentication Protocol for Mobile Environments Found in: Parallel, Distributed, and Network-Based Processing*. Euromicro Conference, (pp. 141-145).
3. Toye, E., Sharp, R., Madhayapeddy, A. & Scott, D. (2005). *Using smart phones to access site-specific services*. IEEE Pervasive Computing, Springer-Verlag, 4(2), 60-66.
4. Daemen, J. & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard.
5. Lamport, L. (1981). Password Authentication with Insecure Communication. *Communications of ACM*, 24(11), 770-772.
6. Mir, N. F. (2007). Computer & Communication Network.
7. Ghogare, S. D., Jadhav, S. P., Chadha, A. R. & Patil, H. C. (2012). Location Based Authentication: A New Approach towards Providing Security. Retrieved from http://www.ijsrp.org/research_paper_apr2012/ijsrp-apr-2012-118.pdf
8. ATM Theft: 8 Tips to Protect Yourself from the 5 Most Common ATM Scams. Retrieved from http://www.scambusters.org/atmtheft.html
9. Authentication. Retrieved from http://en.wikipedia.org/wiki/Authentication
10. Location Manager. Retrieved from http://developer.android.com/reference/android/location/LocationManager.html
11. One-Time Password. Retrieved from http://en.wikipedia.org/wiki/One-time_password
12. Safer Authentication with a One-Time Password Solution. Retrieved from http://msdn.microsoft.com/en-us/magazine/cc507635.aspx#S1
13. What is an ATM? Retrieved from http://www.corpbank.com/uploadedfiles/custom/2_00_350_5385706.pdf