LOCATION BASED AUTHENTICATION USING 4G/5G DEVICES

Seminar report submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF COMPUTER APPLICATIONS

MAHATMA GANDHI UNIVERSITY, KOTTAYAM

By

GINTO SHAJI

Reg no: 190021089255

Under the guidance of

Ms. Jikki Jose

Assistant Professor

Department of Computer Applications

St. Thomas College

Palai, Kerala – 686574

2022

Department of Computer Applications

St. Thomas College, Palai

[Mahatma Gandhi University, Kottayam]

Palai – 686 574, Kerala.

CERTIFICATE

This is to certify that the seminar entitled

"LOCATION BASED AUTHENTICATION USING 4G\5G DEVICES"

Is a bona-fide record of the seminar presented by

GINTO SHAJI(190021089255)

Of sixth semester Computer Applications

In partial fulfillment of the requirements for the award of Degree of

BACHELOR OF COMPUTER APPLICATIONS [BCA]

During the academic year 2021-2022.

Ms. Jikki Jose
Assistant Professor
Department of
Computer Applications

Dr. P. D. George
Head of the Department
Department of
Computer Applications

Internal Examiner

External Examiner

DECLARATION

I hereby declare that the seminar entitled **LOCATION BASED AUTHENTICATON USING 4G\5G DEVICES** submitted by me to St. Thomas College Palai, is a partial fulfilment of the requirement for the award of the degree of Bachelor of Computer Application in Department of Computer Science, is a record of bonafide work done by me under the guidance of Ms.Jikki Jose.

I further declare that the work reported in this seminar will not be submitted, either in part or in full, for the award of any other degree or diploma in this institution or any other institute or university.

Date: GINTO SHAJI

Place: Arunapuram Reg no: 190021089255

ACKNOWLEDGEMENT

This is to express my deepest gratitude to all those who have extended their timely support and helping hands in completing my seminar.

First of all, I am extremely grateful to "**God Almighty**", without whose blessings I could not have been able to successfully complete this seminar.

I express my sincere and profound gratitude **to Rev. Dr. James John** , Principal, St. Thomas College, Palai for providing me all the facilities and encouragement.

Words are boundless to express my sincere thanks to **Dr. P. D. George**, Head of the Department of Computer Application, for giving me an opportunity to present this seminar.

I express my greatest gratitude to **Ms. Jikki Jose,** Assistant Professor, St. Thomas College, Pala for his valuable guidance and encouragement for completing this seminar.

With great enthusiasm I express my gratitude to all the faculty members of Computer Applications Department for their timely help, support and encouragement.

Finally I express my deep appreciation to all my friends and family members for the moral support and encouragement they have given to complete this seminar successfully.

ABSTRACT

Mobile devices 4G/5G have become an important part of our day to day lives. Accessing internet applications has become much easier due to mobile phones. Mobile phones nowadays have been built with new technologies like location based services like GPS. Mobile phones which make it easy to access applications and are the gateway to authentication failure can be used to provide authentication and protect user's private and confidential information. As mobiles have become important for our existence its important have them secured and have them authenticated. Location-based technique is one of the new technologies used to check authentication through smart phones. Authentication is one of the building blocks of security measures and mobile phones can compromise it. For example, if a phone is lost anyone can hack into the phone and get all the confidential information like bank account details and can use the credit card or debit card details. To avoid such scenarios location-based authentication services can be used to collect data and analyze the user's movements and actions. As using internet applications through Smartphones 4G/5G devices has become such a rage, it is necessary to have few methods to help authenticate users.

I intend to survey and give out all the methods which use location services to authenticate users and help in maintaining the security. In this paper, I would like to summarize the methods.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure **Page No**

CHAPTER 1

INTRODUCTION

A password is one of the most common mechanisms used today for authentication, because it can be implemented easily and is cost-effective. Disadvantage of this method is, people generally choose weak passwords and have same passwords for multiple services [1]. As a result of this privacy is compromised and breached, people lose money. Most common solutions fall under three categories :(a) what you know e.g. Passwords, PINS; (b) what you have e.g. tokens, smart cards; (e.g. biometrics like fingerprints, face recognition, palm recognition [1] as you can see in TABLEI. There are many existing systems which use location information to provide solutions for authentication and authorization problems. These systems require a setup, large infrastructures, and specially designed devices. One of the other popular methods is challenge-response where, a challenge is generated by a server to the user's device which calculates a response and sends it back. Other majorly used method is biometrics in which a user provides his identity by a physical feature of the user.

One of the other popular methods are location-based authentication and mobile phone which can be used as a hardware token. We combine these two methods to implement our proposed method. But the main concern with this method is that of privacy. Mobile user's location privacy can be defined in two levels: internally by device or externally by systems and the kind of different networks with which it interrelates [3].

METHODS	**PROCEDURE**
Passwords	Secret combination of characters that can be used several times for login
One-time Passwords	Passwords that are to be used only once
Biometrics	Proves a user's identity by physical features like fingerprints, face recognition
Location-Based	User located in a specificlocationis authorized
Two-factor Authentication	A combination of two types of authentication methods

CHAPTER 2

LOCATION BASE AUTHENTICATION

Authentication can be defined as the process of identifying entities (i.e users) accurately. Location based authentication can be defined as a process of proving a user's identity and authenticity with the help of location detection. Location based authentication has three factors: (a) the individual that wants to be authenticated has to provide a sign of identification (b) user has to have at least one human authentication factor that can be identified even at distinct location (c) distinct location must have some mechanism that can determine the presence of the user at that location.

Privacy Issues

Privacy is defined differently by each individual. Able to come up with one definition is difficult. Privacy is not limited to only human beings, it can be extended to websites. From definition of location based privacy by Beresford and F. Stajano "the ability to prevent other parties from learning one's past or current location. Personal privacy can be categorized into four different categories: (a) Information Privacy (b) Bodily Privacy (c) Privacy of communication (d)Territorial Privacy [3]. Some of the privacy Related issues are:

1. What decides when to let the user know their location- based system is turned on or off? Can it be opt in or opt out approach?
2. Should the information stored be personally identifiable?
3. Should there be information retention period?
4. Can users choose to what extent their information can be personalized?
5. What legal laws are applicable to the users?
6. What level of disclosure is allowed?

Privacy Challenges

Security and Privacy are considered to be the same thing by many people [3]. Security is the action and privacy is a result of a successful action. The first challenge in location based systems is to understand location-based vulnerabilities like leaked personal information from a service like current location or any personal identification details provided they can lead to a lot of trouble for the users and the services in general.

One's current location and some identifying details can help any hacker track the movements of any user and can sometimes reach out to the user's vehicles. Vehicles as privacy vulnerability are a big budding topic today in terms of location-based services.

Usage of Location base Authenticating in Service

Location-based authenticating systems are implemented in real time. Products like iphone, android, visa payment systems etc. use this method for authenticating. Iphone has recently launched a new method to provide security to the device based on the location of the device. Different tolerances can be applied on the device based on the location of it. For example if the device is being used at home it won't need high level security similarly if the device is being used outside then it needs high level security. Mobile phones can be given token provision in which applications can be authenticated by various different methods like over the air(OTA), Bluetooth , SMS request etc.

Launch-key is one of the leading changers in this field. It provides password free logins with a phone in a secure way, security policies, user provisioning, security fencing, analytics etc. Its products can secure any internet-connected application. Mobile app can be used as an authenticator. If a service takes in these products then the user can login without password, will have real time authorization.

CHAPTER 3

.

LOCATION BASE AUTHENTICATION VS LOCATION BASE SERVICES

Program-level services that use location services to control few features can be called location based services. Location based services can be used in Social networking sites, vehicle Tracking, Mobile commerce, Emergency services, Informational services. Location based services generally use control plane locating, GSM localization, self-reported positioning protocols as locating methods. Generally service provider infrastructure determines the location. It replies to user's request based on the location. Example for this is, when user wants to locate the nearest eatery the system has to take the location of the user then has to match with the already there information of the eateries around that area. Location based authentication is used to authenticate users to login or access certain resources based on the location. Location detecting is done by the mobile phone features and sometimes time is taken into account and then the system authenticates the user.

CHAPTER 4

CURRENT APPROACH

Recently there has been a lot of research in this field and a lot has been spoken about its privacy issues and the challenges that a system designer can face while providing an interface to the users due to privacy concerns. Many different methods have been proposed, but most of them need special devices, installation and pre-required knowledge on user's side. we will discuss the various methods proposed in the field of location-based services. Due to internet connectivity and availability of smart phones has enabled users to spend a irrespective of the place and time. This has created a huge challenge for the service providers to authenticate users.

4.1. Generation of Questions

One of the systems implemented is where authentication questions smart phones.Location-based profile are built for all the users based on the data periodically collected like WIFI points the user is connected to.This method was tested on 14 individuals some in sets of two others individually. are generated based on user's location tracked by lot of time over internet User is presented with two sets of questions:one based on the user's own data and the other set chosen randomly[2].
This method implements algorithm based on Bayesian classifier to authenticate legitimate users. First step in this implementation is to calculate user's score for every authentication session, every incorrect option is penalized so that users will not attempt to compromise the system. Following formulas are used (1) ,

Scoreq1 = (P x Lcorrect)-(P x (S - Lcorrect))
Scoreq2 = ((P x Ocorrect)-(P x (S - Ocorrect))
Scoreq3 = ((P x Tcorrect)-(P x (S - Tcorrect))

Note:-

Lcorrect is the number of locations answered correctly. Ocorrect is the number of locations ordered correctly. Tcorrect is number of correctly answered time range. S is number of selected locations [2]

4.2. One time Password (OTP)

The other popular method used by many online services is the usage of one time password(OTP). Services like banking, online transactions, chatting websites etc. use OTP to authenticate users. Any chatting application these days like whatsapp, hike, wechat requests the user to enter the OTP before being able to start the application to make sure that authorized user is only using the application with the given phone number. A volatile password can lower the risk of passwords being stolen, shoulder surfing, phishing etc. GPS nowadays is precise and this ca help implement this method without any problem. This method is comparatively easy to implement when compared with other methods. This method requires only the in-built GPS system and no special designs or interfaces which makes it cost effective. OTP is generated based on time and location which will be difficult for the hackers to know the exact details. In-case of a misjudgment where a legal user is not allowed to access the service, SMS service can be used. Following procedure is followed and checks TABLEII for notations:
The table shows the GPS system using nowadays as shown by the formula:

$$Skey(Pkey(IMSI||OTP)) \rightarrow IMSI||OTP \rightarrow OTP \rightarrow f(OTP) \rightarrow T,(x,y)$$

Table II Notations

PKey	Public key
SKey	Secret Key
IMSI	International Mobile Subscriber
||	Concatenation

4.3. Policy Beacon

A small device called policy beacon is placed in an area to draw a boundary in which the policy is in effect. It has an area location service discovery implementation and it can be used by mobile devices. If mobile devices are equipped with policy beacons protocol then they will be able to sense the active policy beacons in that area. Footprint of the beacon's communication signal determines whether the device is in the vicinity or out. Policy Beacon authentication mechanism checks the proximity of the policy beacon on a mobile device. If a device is been able to be detected and verified it is considered successful. It has the following disadvantage: Policy settings may affect the availability of the functionality on the mobile devices.

Two Factor Authentication

This method follows two factor authentications which means it has two different authenticating mechanisms combined together. Here location and Biometric are combined.GPS tracking is used to know the location of a particular user.GPS gives longitude and latitude coordinates and send them to the local server for authentication [5].Fingerprint is used as the biometric here. Fingerprint identification algorithm is used. This method uses encryption for exchange of data after authentication. (Drawbacks: It has to worry about all the data security problems and has to increase the strength of the security protocols used.)

Location Registration

This protocol has two level implementation. In the first level registration algorithm is used. Registration by users is allowed only once, when the user is joining the system. Next level is authentication. Authentication is performed for every session unlike registration phase. In this protocol, two types of location information is taken- static and dynamic location information. Static location information has the standard/static location that was captured during registration and is stored in location based ID database. This location information is not changed till the user explicitly changes it. Dynamic location Information is gathered when the user requests for the authentication. Here authentication server sends some authenticating challenges to the users when they want to access the system. User

responds to the challenge by giving the security credentials. On success of this step the authenticating server sends location verification request to the location based client application, which resides on the user's smart-phone. User is prompted to enter the PIN and then this PIN is sent to location based ID database and encryption is performed. Location authorization policy sends the result to the server and then finally authenticating server authenticates the user [21]. Disadvantages of the protocol are:

1. PIN can be stolen
2. Security credentials with which the user responds can be stolen too

CHAPTER 5

BEST APPROACH

As there are various methods to implement location-based authentication using smart phones it becomes important to take advantages and disadvantages of each method into consideration.

The other method that can be used is based on question generation. As this method uses Bayesian approach and questions it is very much precise. But the biggest disadvantage of this method is that anyone can pretend to be that user and answer the questions. As there are no proper identification details available, others can act like an authorized user. But this method has a strong encryption technique.

Typically OTP can be generated by using physical features like login time that helps us detect the location. It is assumed that already all the users are registered with the application server. We make an assumption that forms the base of this method that mobile clock and application server clocks are synchronized. After the mobile device initiates the process and gives it location and time it gets recorded in the server, then the velocity of the device is calculated. Then

Phase I: Location & Time based Authentication See Table 2 for Notations

Step 1: Mobile device is initiated by the user then, it sends current time T_0, IMSI and location L to the server. Location $L(X_0,Y_0)$ and time are sent to the application server and the data is recorded in database as shown in Fig. 1.

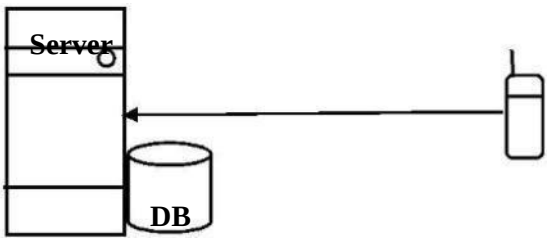


Fig.1. Mobile sends IMSI, Location L and time t0, encrypted by public to the server

Step 2: After a time period, New Time Period and location $L(X_1,Y_1)$ are sent by the mobile device to the application server which stores it in database.

Step 3: The server calculates the velocity of the mobile device subsequently, by the following formula (2),

$$\mathbf{V=\sqrt{(X_1-X_0/T_1-T_0)^2 + (Y_1- Y_0 / T_1- T_0)^2}} \quad \mathbf{(2)}$$

Step 4: After referring the statistics in [4], it is probable to predict the future moving direction and the mobile device location.

Step 5: The distance d can be derived from steps 3 and 4. As in (3),

$d = Vt\ \Delta T$ (3)

On the basis of the algorithm given in [4], a line is passed through the two locations $L(X_0,Y_0)$ and $L1(X_1,Y_1)$. The given line has the formula y=ax+b. The equation is used to calculate a and b as in (4),

$$\begin{aligned} a &= \\ b &= \end{aligned} \quad \begin{cases} a = Y_1-Y_0 / X_1-X_0 \ , X_1 \neq X_0 \\ b = X_1Y_0 - X_0Y_1 / X_1-X_0 \end{cases} \quad (4)$$

An equilateral triangle is made with one point at (X_1, Y_1) and center on line l. The equilateral triangle's edge length is d. Also, the equilateral triangle's center coordinate (X, Y) is calculated by using the formula below in (5),

$$CxX1\ \frac{\sqrt{3}d\ X1X0\ COS(\tan\text{-}1(|a|))}{3|X1X2}, \quad (5)$$

$$CyY1\ \frac{\sqrt{3}dY1Y0\ \sin(\tan\text{-}1)(a))}{6|Y1Y0}$$

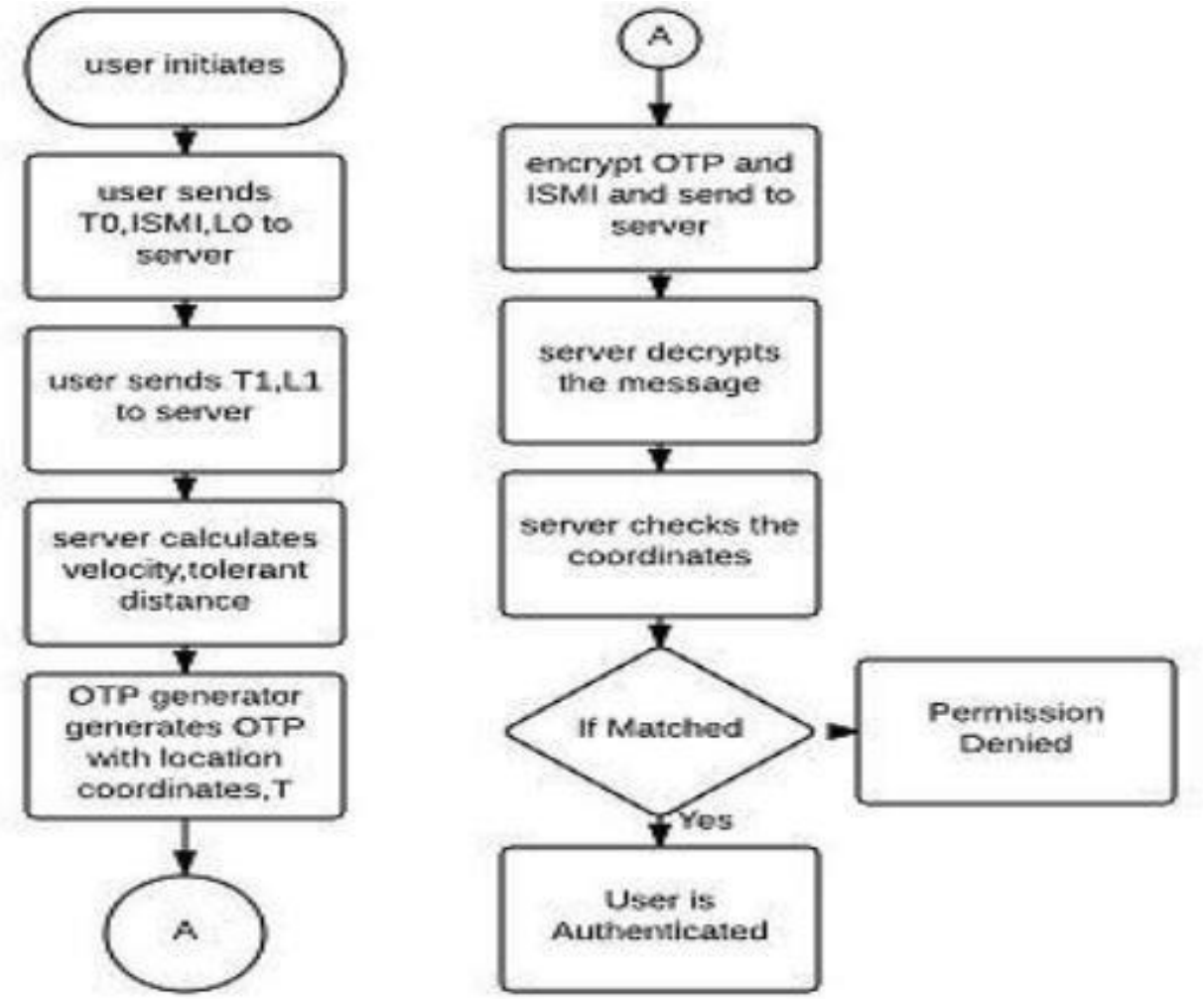
Step6: By using the location received from the GPS and current time t, is used to generate the OTP when user want to login into the application server.

Step7: OTP and IMSI together will be encrypted by the public key and is sent to the server.

Step8: Encrypted message received by the server is decrypted by the shared key. Location L(X,Y) is extracted by the server with the OTP from the message. Time t can be extracted from the inverse function f().

Step9: Now the server checks if the location coordinates(X,Y) are in the tolerant distance. If the coordinates match then the user is authenticated or else is not permitted.

The flow chart shows the whole steps using in authentication process as given below:



Phase II: Supplementary SmS based mutual Authentication

In case where the coordinates are not in the range of tolerant distance or in case of failure of method one, SMS based authentication is used so that genuine user can login.

Step1: User is assumed to be registered already in the system before he seeks permission to login. A smart card is inserted in the mobile phone which helps user request and get OTP. As user has an account already, he will possess the password as well.

Step2: Meanwhile, the system selects two large prime numbers and find modulo p.

Step3: When the user needs OTP then the user inserts smart card into the mobile phone and enters the account details and the password and a large prime number less than A circle is drawn which contains an equilateral triangle and shares same center(CX,CY). Then we get the predicted future location.(P-1). The system acquires the time stamp . XOR operation is performed and value C is calculated, now the device sends the message M (time stamp, account details, C) via SMS to the server.

Step4: If the time stamp has been used already the request is terminated. The account details inserted by the user are matched with the details in authentication database. The server then calculates by choosing another prime number y less than (P-1) and is sent to the device via SMS.

Step5: The device checks if the sent time stamp is equal to the stored time stamp. If not, the error message is generated.

Step6: Mobile device computes OTP

Step7: Input the OTP to the server

Step8: Server checks if the received OTP and time stamp matches the stored time stamp and the OTP.

Step9: If the two fields match then the user is authenticated.

Advantages

OTP mechanism is the best mechanism that can be used to authenticate users based on location. Advantages of this method are:

a. Due to their volatile nature, it becomes difficult for the hackers to get the information.

b. It not only gives time dependent but also location dependent OPT that makes it impossible for the hacker to know the exact location and it can't be reused.

c. To improve the precision, it uses developed statistics.

	Traditional Authentication System	**OTP system**
Inputting Accounts and Passwords	Required	Not Necessary
User Behavior Dependant	No	Yes
Passwords Lifetime	Permanent	Volatile

Different Implementations of OTP

Based Mechanism: OTP once generated will be valid for certain period of time if certain conditions are met.

Time Based Mechanism: OTP once generated will be valid for some period of time.

Time and Event Driven Mechanism: Combination of both time and event based mechanisms

Security Conditions

Event condition specified in the above stated best approach (OTP) is the tolerant area. Mimicking of the user's velocity and exact behavior is very difficult. Table4 gives a good view of the security value of the OTP method compared to existing methods.

Protocol	**Kerberos**	**S/Key OTP**	**Best Approach OTP**
Reply Attack	√	√	√
Eavesdropping Attack	ŏ	√	√
Dictionary Attack	×	√	√
Brute Force Attack	×	ŏ	√
Man in the Middle Attack	×	×	√
User Impersonation Attack	ŏ	√	√

CHAPTER 5

CONCLUSION

Mobile phones have garnered a lot of popularity but security of mobile phones has always a debatable point. Location based Authentication systems have helped in reducing security, privacy concerns. Europay Master Card Visa Chip Authentication Program has been using these protocols. Most of the protocols are time-constrained .Still there is a lot of improvement that can happen and protocols can be much stronger. We surveyed almost all the existing protocols of Location based Authentication Systems and concluded that usage of OTP generation is one of the best methods to solve the authentication problems and is easy and effective to implement. We also surveyed about the usage of these protocols in real time environment. Usage of Location based Authentication systems are much better than the traditional password system and we have provided the reasons for it in this paper.

CHAPTER 7
REFERENCES

[1] David Jaros and Radek Kuchta, New Location-based Authentication Techniques in the Access Management,
2010th International Conference on Wireless and Mobile Communications
[2] Yusuf Albayram, Mohammad Maifi Hasan Khan, Athanasios Bamis,Sotirios Kentros,Nhan Nguyen and Ruhua Jiang, A Location- Based Authentication System Leveraging Smartphones 4G/5G, 2014 IEEE 15th International Conferemce on Mobile Data Management
[3] Amit Kumar Tyagi,N.Sreenath, Future Challenging Issues in location-based services, International Journal of Computer Applications Volume 114-No 5. March 2015.
[4] Wen-Bin Hsieh and Jenq-Shiou Leu, Design of a Time and Location Based One-Time Password Authentication Scheme.
[5] Shradha D. Ghogare, Swati P. Jhadav, Ankitha R, Hima C. Patil, Location Based Authentication:A New Approach towards Providing Security, International Journal of Scientific and Research Publication,Vol 2, Issue 4, April 2012
[6] L.Scott and D.Dennings, Geo-encryption Using GPS to Enhance Data Security, GPS world,pp.40-49,2003.
[7] Hsien Chou Liao, Yun-Hsiang Chou, A New Data Encryption Algorithm Based on the Location of Mobile Users, Information Technology journal,vol 7, issue 1,pp 63-69,2008.
[8] D.Son, A.Helmy, B.Krishnamachari, The Effect of Mobility- induced Location Errors on Geographic Routing in Ad Hoc and Sensor Networks:Analysis and Improvement using Mobility Prediction, IEEE Transactions on Mobile Computing,Vol 3, Issue 3, pp.233-245,July 2004.
[9] "One Time Password", http://us.zyxel.com/
[10] "Ukey", http://ukey.com.tw/site/ukey.html [11] Mohhamed Hussain , An Authentication Scheme to Protect the Location Privacy of Femtocell Users, IEEE 978-1-4-799-- 7100-8/14 2014.
[11] Liang Hua , J iazhu Dai, A Location Authentication Scheme Based on Adjacent Users, IEEE 2014.
[12] Min-Hsao Chen, Ching- Han Chen, Secondary User
Authentication based on Mobile Device Location, 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage.
[13] Jaoquin Torres, Jose M. Sierra, Antonio Izquierdo, A Realistic Approach on Password-Based Mutual Remote Authentication Schemes with Smart-cards, Digital Ecosystems and Technology Conference, pp. 334-338,2007.
[14] Huixia Jia, Li Tu, Gelan Yang, Yatao Yang, An Improved Mutual Authentication Schemein Multi-Hop WiMax Network, International Conference on Computer and Electrical Engineering, pp. 296-299, 2008.
[15] William Su, Sung-Ju Lee, Mario Geria, Mobility prediction in wireless networks, st Century Military Communications Conference Proceeding, vol. 1, pp. 491-495, 2000.
[16] Lei Mu, Geng-Sheng Kuo, Ningning Tao, A Novel
Location Algorithm Based on Dynamic Compensation Using Linear Location Prediction in NLOS Situations, Vehicular Technology Conference Proceeding, Vol. 2, pp. 594-598, 2006.
[17] Philip Hoyer, OTP and Challenge/Response algorithms for financial and e-government identity assurance: current landscape and trends, ISSE, 2008
[18] Whitefield Diffie, Martin Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Vol. 22, Issue 6, pp- 644-654, Nov. 1976.
[19] S.von Watzdorf and F.Michahelles, Accuracy of Positioning Data on Smartphones 4G/5G, 2010, pp. 1-4.

[20] Feng Zhang, Aron Kondoro, Saed Muftic, Lpcation based Authentication and Authorization using Smartphones 4G/5G, 2012 IEEE Conference on Trust, Security and Privacy in Computing and Communication.