



ICONI



KOREAN SOCIETY FOR INTERNET INFORMATION

The 11th International Conference on Internet

(ICONI 2019)

Dec. 15-18, 2019, Lotte Hotels & Resorts Hanoi, Vietnam

<http://www.iconi.org>

Proceedings of ICONI 2019

| Organized by |

Korean Society for Internet Information (KSII)

| Sponsored by |

Korea Electronics Technology Institute (KETI)

Contents

13-1	Bug Bounty Regulatory and Institutional trends DaUn Jung, JungTaek Seo (Soonchunhyang Univ., ROK)	388-390
13-2	Fingerprint and Location based Authentication Scheme in Cloud Environment Jeong-Seok Jo, Jin Kwak (Ajou Univ., ROK)	391-396
13-3	A Study on the Possibility of Cyber Attack by the Intrusion of Drone into Infrastructure JangHoon Kim, JooChan Lee, MinGyu Lee, JungTaek Seo (Soonchunhyang Univ., ROK)	397-399
13-4	Utilizing Classification-based Fault Pattern for Enhancing the Effective Search of GP Kyeongsic Min, Ji-Su Choi, Byungjeong Lee (Univ. of Seoul, ROK)	400-402
13-5	Memory Modulation Attack through PLC Vulnerability JooChan Lee, HyunPyo Choi, JangHoon Kim, JunWon Kim, DaUn Jung, JiHo Shin, JungTaek Seo (Soonchunhyang Univ., ROK)	403-405
13-6	The Affection Management of Massive Traffic Based on MEC and Network Slicing Method for Improving 5G Core Network Performance Zilong Jin (Nanjing Univ. of Information Science and Technology, China), Jin Wang, Wenbing Wu, Yongsong Zou (Changsha Univ. of Science & Technology, China)	406-408
14-1	A Research on Data Block Value-Modulated Attack Techniques through Siemens S7 PLC Vulnerability Jun-Won Kim, Hyun-Pyo Choi, Joo-Chan Lee, Jang-Hoon Kim, Da-Un Jung, Jung-Taek Seo (Soonchunhyang Univ., ROK)	409-412
14-2	Small sample time series prediction based on multi-model fusion method Xi Chen, Yuming He, Dun Cao, Jie Li, Shuo Peng (Changsha Univ. of Science & Technology, China)	413-417
14-3	A Compositional Approach to Generate Benign Samples from Android Packages Ngoc-Tu Chau, Souhwan Jung (Soongsil Univ., ROK)	418-423
14-4	The Segmentation of Psoriasis Area with Level Set HyunJong Yoo, JiWon Lee, Moon Choi, EunBin Kim (Soonchunhyang Univ., ROK), YooSang Baek (Korea Univ., ROK), OnSeok Lee (Soonchunhyang Univ., ROK)	424-427

Fingerprint and Location based Authentication Scheme in Cloud Environment

Jeong-Seok Jo¹ and Jin Kwak²

¹ISAA Lab., Department of Computer Engineering, Ajou University
Suwon, South Korea

²Department of Cyber Security, Ajou University
Suwon, South Korea

[e-mail: jsjo.isaa@gmail.com, security@ajou.ac.kr]

*Corresponding author: Jin Kwak

Abstract

Cloud networks are used to provide a variety of services for various users. As the services provided using cloud networks have expanded, the number of service users has increased. Accordingly, various resources of users exist in the clouds, and the importance of user authentication to obtain access to resources has increased. Furthermore, as many problems of authentication schemes using ID/PW have been pointed out, the need of authentication schemes using additional factors to enhance ID/PW has increased. Therefore, this paper proposes a user authentication scheme employing fingerprint and GPS-based location information along with user ID/PW and analyzes the security of the proposed authentication scheme.

Keywords: Cloud, Authentication, Fingerprint, GPS

1. Introduction

Recently, services provided by using cloud networks have expanded in diverse areas. According to Oracle's "Cloud Computing in Financial Services", that cloud services can be used in financial sector, and specifically, it can be used in Banking, Insurance and Analytics areas[1]. Furthermore, according to Gartner's "Gartner Top 7 Security and Risk Trends for 2019, many companies have emphasized the importance of cloud platform security as they expand their service offerings using cloud platforms[2].

Due to such emphasis made on the importance of cloud platform security, consideration of authentication in cloud services

has also become crucial. Oracle expected a new form of authentication to replace the password in authentication[3], and Gartner expected greater use of biometric authentication[4]. Andre van Clif et al.'s also suggested the importance of performing authentication, including user physical location information, to mitigate vulnerabilities to access control through logical authentication schemes[5].

Therefore, this paper propose an authentication scheme using biometric information, namely, a fingerprint, and location information for physical access control in the cloud environment.

2. 2. Related Work

2.1 Shraddha D. Ghorgare et al.'s scheme

Shraddha D. Ghorgare et al., in their study “Location Based Authentication: A New Approach towards Providing Security,” proposed a simple authentication system using ID/PW, fingerprint information, and location information. The proposed authentication system consists of the registration and login phases, and the sequence of operation is as follows [6].

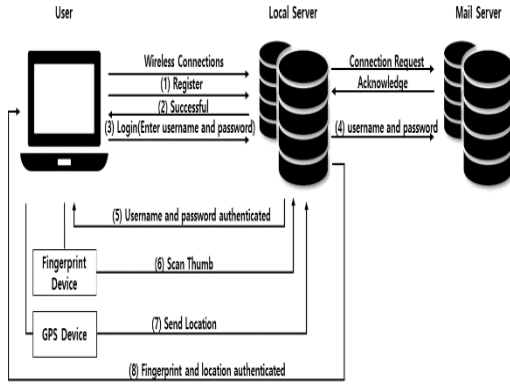


Fig. 1. Shraddha D. Ghorgare's Scheme

1) Registration Phase

Step 1. Enter User ID and Password

Step 2. Scan fingerprint

Step 3. Select possible locations from database

Step 4. Validate and store data

2) Login Phase

Step 1. Enter User ID and Password and validate it.

Step 2. If success, scan fingerprint

Step 3. If success, implicitly check location

Step 4. If success, grant access

As such, Shraddha D. Ghorgare et al.'s presented a simple authentication system using fingerprint and location information.

2.2 Kim's Scheme

In the study “Security Enhanced Dynamic ID based Remote User Authentication Scheme for Multi-Server Environment” Jun-Sub Kim et al.'s proposed an authentication scheme in a multi-server environments. The proposed authentication scheme consist of registration and

login steps, and performs authentication via a user's ID, Password(PW), random number, and server's random number and key.

In the registration phase of the proposed scheme, the values $A_i = h(h(ID_i || PW_i) || h(b^*PW_i))$, $B_i = h(x || ID_i)$, $D_i = h(ID_i || PW_i) \wedge h(B_i || h(x || y))$ and $E_i = B_i \wedge h(x || y)$ generated by logical operations using ID_i , $h(ID_i || PW)$, $h(b^*PW_i)$ are used.

In the login phase of the suggested scheme, the values $C_1 = h(SID_j || h(y)) \wedge N_i$, $C_2 = h(h(SID_j || h(y)) || N_i) \wedge E_i$, $C_3 = h(E_i || h(SID_j || h(y)) || N_i) \wedge D_i$, $C_4 = h(h(b^*PW_i) || CID_i || D_i || E_i || N_i)$, $C_5 = h(b^*PW_i) \wedge N_i \wedge N_j$, $C_6 = h(h(b^*PW_i) || h(ID_i || PW_i) || SID_j || N_i)$, $C_7 = h(h(b^*PW_i) || h(ID_i || PW_i) || SID_j || N_j)$ are used.

Specific sequence of operations is as follows[7].

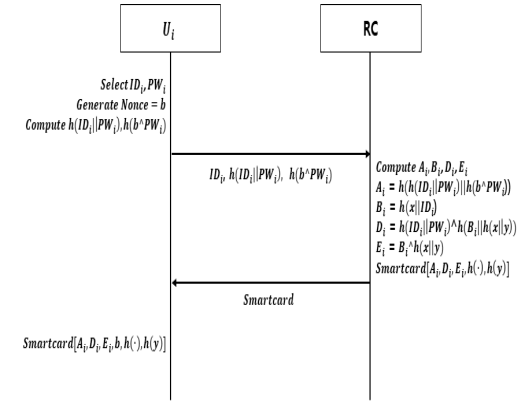


Fig. 2. Kim's Scheme Registration Phase

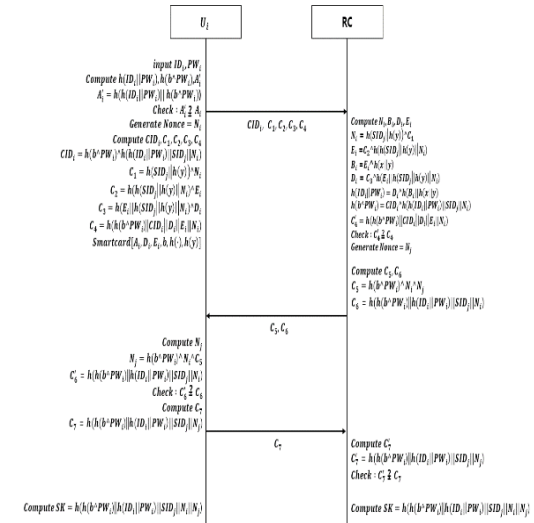


Fig. 3. Kim's Scheme Login Phase

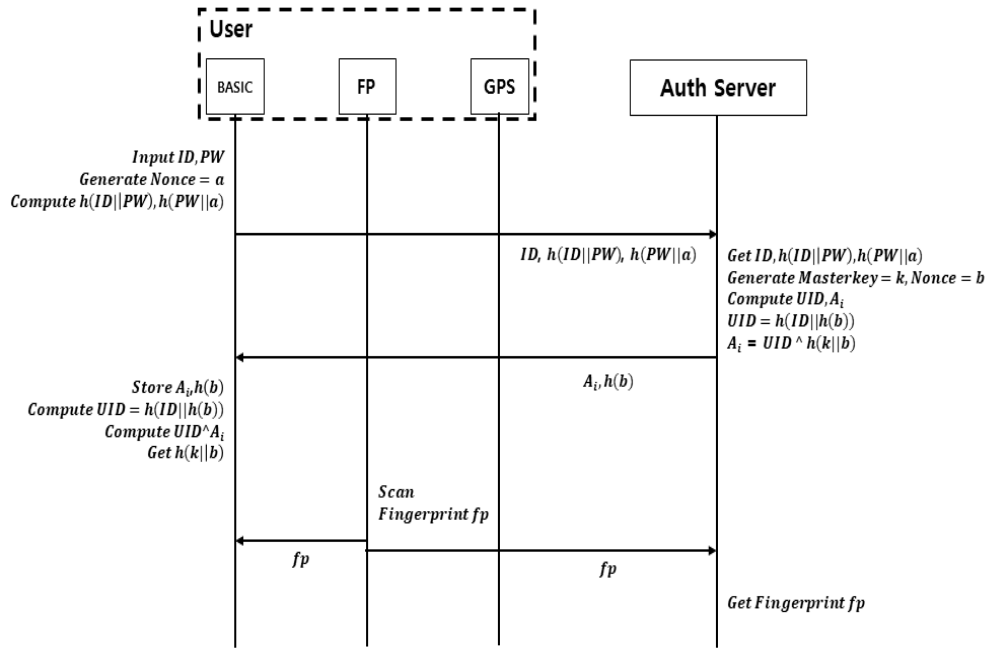


Fig. 4. Registration Phase

3. 3. Proposed Scheme

By using fingerprint information, authentication is possible through fingerprint, which is a special value of the user, and is resistant to Guessing Attack[8]. Furthermore, everyone has unique fingerprint information, therefore, a system can identify respective objects [9] and deal with problems such as leaking and forgetting PW, which are vulnerabilities of the ID/PW-based authentication scheme [10].

As the location information is used, PW/Current Location two information is required, making it difficult to attack, and generating keys through various combinations of information, including PW/Current Location[11]. In addition, vulnerabilities such as weak PW selection in ID/PW-based authentication schemes can be coped with[12], and location-based physical access control can mitigate threats such as access bypass using logical access control security vulnerabilities[5].

Based on these characteristics, we would like to suggest authentication schemes in the cloud environment using fingerprint and location information.

3.1 Fingerprint and Location based Authentication Scheme

In this paper, we propose a fingerprint and location information-based authentication scheme to be used in the cloud environment. It is constructed based on the concept of the registration and login phases of the system proposed by Shraddha D. Ghorgare et al. in their study, as described in Section 2.1.

The authentication scheme proposed in the present paper consists of a basic module that performs the basic computation of a user information, an FP module that collects the fingerprint information, a GPS module that collects the location information, and an authentication server that performs the authentication. Furthermore, this scheme performs the registration and login phases. The detailed process of authentication is provided in the following subsection.

3.1.1 Registration Phase

● Step 1. Input ID, PW

In the user's basic module, ID and PW are entered and a random number a is generated. Furthermore, this value is used to generate $h(ID||PW)$, $h(PW||a)$.

● Step 2. Send Credential Parameter

User's Basic module sends ID,

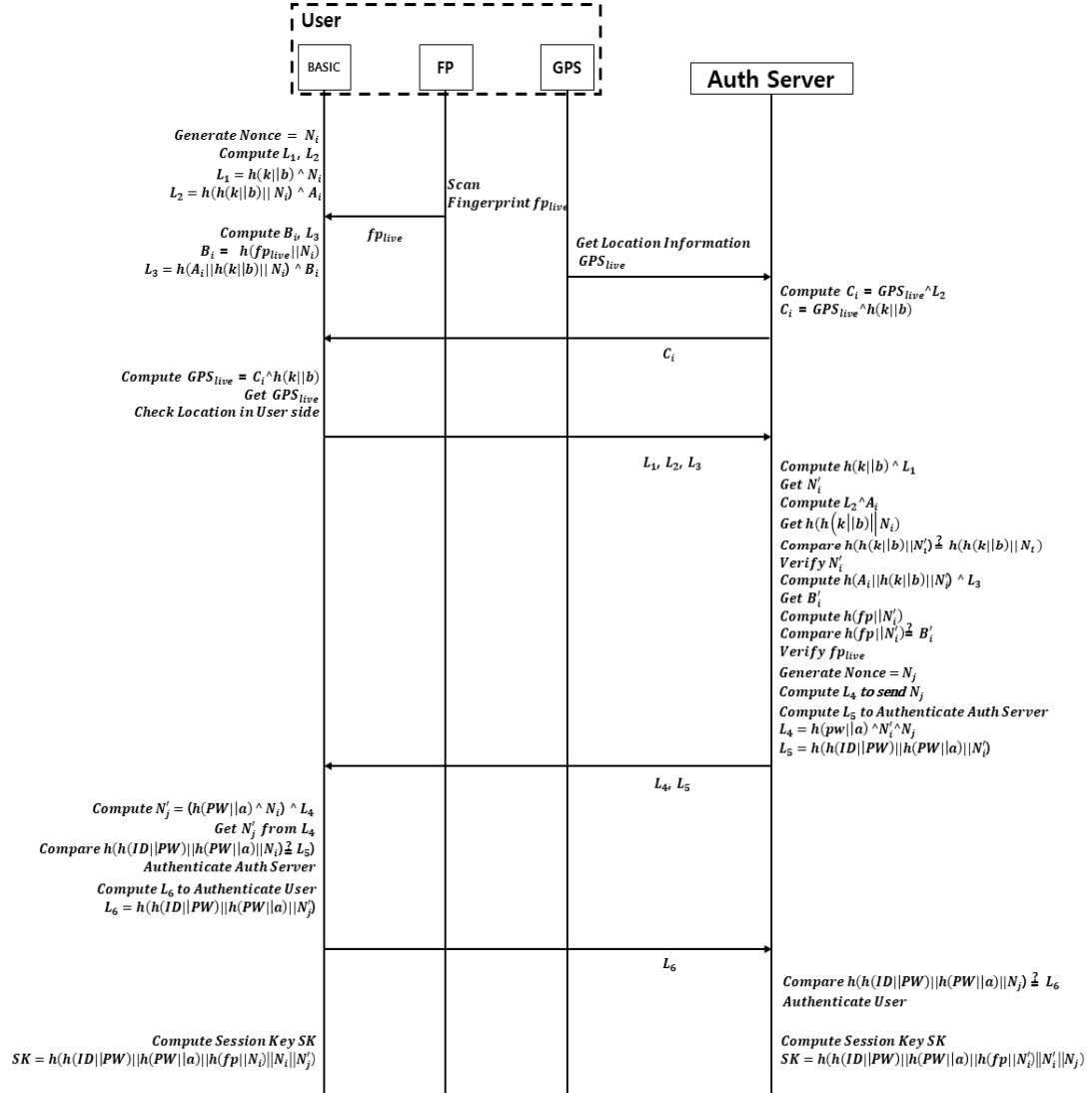


Fig. 5. Login Phase

$h(ID||PW), h(PW||a)$ values to Auth Server.

- **Step 3. Compute A_i, UID**

Auth Server generates Masterkey k , random number b . Use these values to compute $UID = h(ID||h(b))$, $A_i = UID \wedge h(k||b)$ and send $A_i, h(b)$ values to the Basic module of the user.

- **Step 4. Get Auth Server's Parameter**
User's Basic module stores $A_i, h(b)$, and computes the UID to obtain the parameter $h(k||b)$, which is the auth server's parameter.

- **Step 5. Scan Fingerprint**

User's FP module obtains the fingerprint information(fp) of the User and sends it to the Basic module of the User and to the Auth server.

- **Step 6. Get Fingerprint**

Auth Server obtains fp , which is the fingerprint information of the User.

3.1.2 Login Phase

- **Step 1. Compute User's Parameter**

User's Basic module generates random number N_i and computes parameters $L_1 = h(k||b) \wedge N_i$, $L_2 = h(h(k||b)||N_i) \wedge A_i$.

- **Step 2. Scan Fingerprint**

User's FP module obtains the User's fingerprint information fp_{live} and sends fp_{live} to the User's Basic module.

● **Step 3. Compute User' s Fingerprint Parameter**

User's Basic module generates $B_i = h(fp_{live} || N_i)$, $L_3 = h(A_i || h(k || b) || N_i) \wedge B_i$ using the received fp_{live} .

● **Step 4. Get User' s GPS Information**
User's GPS module sends GPS information GPS_{live} to the Auth Server.

● **Step 5. Compute User' s GPS Parameter**
Using the received GPS_{live} , the Auth Server computes $C_i = GPS_{live} \wedge h(k || b)$ and sends C_i to the User's Basic module.

● **Step 6. Verify User' s GPS Parameter**
User's Basic module obtains GPS_{live} through $GPS_{live} = C_i \wedge h(k || b)$ and verifies if the User is in a legitimate position.

● **Step 7. Send User' s Parameter**

User's Basic module sends the computed L_1, L_2, L_3 .

● **Step 8. Verify User' s Parameter**

- ① Auth Server obtains User-generated N'_i through the operation of $h(k || b) \wedge L_1$
- ② Auth Server obtains $h(h(k || b) || N_i)$ through the operation of $L_2 \wedge A_i$.
- ③ Auth Server computes $h(h(k || b) || N'_i)$ using N'_i obtained in ① and compares it with $h(h(k || b) || N_i)$ obtained in ②.
- ④ Auth Server obtains B'_i through the operation of $h(A_i || h(k || b) || N'_i) \wedge L_3$
- ⑤ Using fp and N'_i obtained in the registration phase, compare $h(fp || N'_i)$ and B'_i to verify the fingerprint information of the User.

● **Step 9. Compute Auth Server' s Parameter**

Auth Server generates random number N_j and $L_4 = h(pw || a) \wedge N'_i \wedge N_j$, $L_5 = h(h(ID || PW) || h(PW || a) || N'_i)$. Send the generated L_4, L_5 values to the User's Basic module.

● **Step 10. Authenticate Auth Server**

- ① User's Basic module obtains N'_j through the operation of $(h(PW || a) \wedge N_i) \wedge L_4$
- ② User's Basic module computes $h(h(ID || PW) || h(PW || a) || N_i)$ and authenticates the Auth Server by comparing it with $L_5 = h(h(ID || PW) || h(PW || a) || N'_i)$ received from **Step 9**.

● **Step 11. Compute User' s Authentication Parameter**

User's Basic module computes the User's authentication parameter $L_6 = h(h(ID || PW) || h(PW || a) || N'_j)$ and sends it to the Auth Server.

● **Step 12. Authenticate User**

Auth Server computes $h(h(ID || PW) || h(PW || a) || N_j)$ and authenticates the user by comparing it with $L_6 = h(h(ID || PW) || h(PW || a) || N'_j)$ received by **Step 11**.

● **Step 13. Generate Session Key**

User's Basic module and Auth Server each generate the same Session Key SK using the values each have. The User's Basic module computes $SK = h(h(ID || PW) || h(PW || a) || h(fp || N_i) || N_i || N'_j)$ and Auth Server computes $SK = h(h(ID || PW) || h(PW || a) || h(fp || N'_i) || N'_i || N_j)$, and the User and the Auth Server can obtain the same Session Key.

3.2 Security Analysis of Proposed Scheme

In this section, the security analysis is performed for the authentication scheme proposed in section 3.1.

Backward Secrecy: Even if an attacker knows Auth Server's master key x , it cannot know the random number used in the previous session. Therefore, it is impossible to generate a Session Key SK identical to that of the previous session.

Replay Attack: Even if an attacker resends L_1, L_2 , and L_3 in **Step 7**, authentication cannot be performed because L_6 using the server's new random number N_j cannot be computed.

Spoofing Attack : Even if an attacker obtains L_1, L_2, L_3 from Step 7., it is difficult to acquire the value because the attacker can not know $h(k || b)$.

Mutual Authentication : Perform mutual authentication of the User and Auth Server through L_5, L_6 values from **Step 9. ~ 12**.

Forward Secrecy : Even if the attacker knows the Session Key : SK of the previous session, it cannot know the key that will be generated next because N_i, N_j are generated at every login operation.

4. Conclusions

This paper proposed an authentication scheme using the fingerprint and location information for user authentication in a cloud network. The proposed authentication scheme performs the user authentication in the cloud environment, which has been widely used in recent years. This authentication scheme employs not only ID/PW but also the user's fingerprint and location information, which can be used in multi-factor authentication. It utilizes the fingerprint information to mitigate security threats such as guessing attack, which can occur in the user PW-based authentication scheme. In addition to such logical access control, an enhancement of the authentication scheme incorporating the current location information is proposed, thereby, providing physical access control.

Furthermore, the security analysis of the proposed authentication scheme was performed with respect to the backward secrecy, reply attack, etc.

The proposed authentication scheme performs the user authentication through an authentication server. In reality, however, many cloud servers exist to provide cloud services. Therefore, the future study will focus on developing the fingerprint and location information-based authentication with the use of multiple cloud servers.

5. References

- [1] Oracle, "Cloud Computing In Financial Services : A Banker's Guide", Nov. 2015.
- [2] Gartner, "Gartner Top 7 Security and Risk Trends for 2019", Jun. 2019.
- [3] Oracle, "Oracle and KPMG Cloud Threat Report 2019", Nov. 2018.
- [4] Gartner, "Predicts 2019: Identity and Access Management", Dec. 2018.
- [5] Andre van Cleeff, Wolter pieters, Poel Wieringa, "Benefits of Location-Based Access Control : A Literature Study", Proceedings of the 3rd IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSSCom 2010)., pp.739-746, 2010.
- [6] Shraddha D. Ghorgare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, "Location Based Authentication : A New Approach towards Providing Security", International Journal of Scientific and Research Publication, Vol. 2, No. 4, Apr. 2012.
- [7] Jun-Sub Kim, Jin Kwak, "Security Enhanced Dynamic ID based Remote User Authentication Scheme for Multi-Server Environments", Internet Journal of u- and e-Services, Science and Technology, Vol. 8, No. 7, pp.127-136, Jul. 2015.
- [8] Sangeeth Kumar.S, R.Venkatesan, "Ranking of Authentication Schemes based on Critical Limiting Factors", International Journal of Computer Applications, Vol. 92, No.7, pp34-40, Apr. 2014.
- [9] Julian Fietkau, Starbug, Jean-Pierr Seifert, "Swipe Your Fingerprints! How Biometric Authentication Simplifies Payment, Access and Identity Fraud", in Proc. of 12th USENIX Conference on Offensive Technologies, Aug. 2018.
- [10] Wencheng yang, Song Wang, Jiankun Hu, Guanglou Zheng, Craig Valli, "Security and Accuracy of Fingerprint-Based Biometrics: a Review", Symmetry 2019, Vol. 11, No. 2, Jan. 2019.
- [11] Torben Kuseler, Ihsan Alshagib Lami, "Using Geographical Location as an Authentication Factor to Enhance mCommerce Applications on Smartphones", International Journal of Computer Science and Security(IJCSS), Vol. 6, No. 2, pp.277-287, 2012.
- [12] Feng Zhang, Aron Kondoro, Sead Muftic, "Location-based Authentication and Authorization Using Smart Phones", in Proc. of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, pp.1285-1292, 2012.