Journal of Excellence in Computer Science and Engineering, Vol. 4(1) 2018, pp. 1-10

RESEARCH ARTICLE

# Reliable Application Enhanced Framework (RAEF) for Frenzie Application upon a Frenzy Cloud Overlay Architecture for Presence Services using Biometrics through Smartphones

***A Antush Agnes[1]**

[1]Independent Researcher, Antush Casilda, Kunjaluvilai, Arumanai, Tamil Nadu, India.

Received- 20 July 2017, Revised- 20 October 2017, Accepted- 14 December 2017, Published- 22 January 2018

**ABSTRACT**

People have started using social networking as a place where they can communicate with whomever they wish, irrespective of their residences. It is a must to have a protected, reliable, authenticated, robust and secured framework by taking all the aspects that could encompass the overall functioning of the social network in a superior way. Social networking has to provide security features to build a reliable architectural framework that will form a foundation stone in creating an application, which facilitates the security aspects and ensures the privacy of the application users. The present work intents to create an architectural framework named RAEF (Reliable Application Embedded Framework) supporting the Online Social Network (OSN) application "Frenzie" that could embed a safer authentication scheme in terms of user authentication without password. Additionally, biometric based authentication scheme and an overlay architecture coined as Frenzy Cloud are used to reduce the load and to address the scalability issue.

**Keywords:** Social Network, RAEF, Frenzie, Bio-metric based authentication, Frenzy Cloud.

## 1. INTRODUCTION

Social media is a convolution of computer mediated technologies that holds multimedia contents like images, texts, etc., that could be made visible to anyone in the world, who can share, edit and post their ideas so that their ideas could be spread world-wide. Social media is entirely different from other media like newspaper, television channel, etc. in the aspect that the communication which is involved is of single side. It also finds its place prominent in terms of instant chatting within a group of people whom they feel to share their ideas in a private manner [1].

### 1.1. Authentication

User authentication in Online Social Network (OSN) application is a major process, which promotes integrity to any application that involves communication between people through online means. This forms the basic step of every OSN application, which makes the chat process encountered by the person to be highly secured. If not given utter importance to authentication process, it will affect the reputation of application. Framing a good authentication procedure in maintaining the integrity of an authenticated person is a better choice.

The two major activities that take place during authentication are,

- Identifying the identifier in specific.
- Verifying by associating the exact person to his identifier.

As authentication is a methodology which forms the basic step for a person to gain authority over the control of a computer system, if the person is not been precisely verified, unauthentic access could possibly steal the authenticity of the authorized access. Several approaches adopted for user authentication are shown in figure 1.

*Corresponding author. Tel.: +917502399050
Email address: antush7agnes.researcher@gmail.com (A.A.Agnes)
Double blind peer review under responsibility of DJ Publications
http://dx.doi.org/10.18831/djcse.in/2018011001


Figure 1.User authentication approaches

- Something you know:

  A well-known example for this approach is passwords. The passwords that are used in our day today life fall under this category of "something you know". But there is also a chance for "something we know" to turn out to be "something we forgot". When we note down passwords to remember it, there is a worse situation that "something you know" to become "something others know". Thus the passwords possess a major security threat. So, passwords are not up to the mark in terms of authentication procedures. Another example includes pin number.
- Something you have:

  This strategy of human authentication resolves issue of "something we known to be forgotten". But this strategy involves the situation that the user must have some object to authenticate with. Here also problem arises when the object may be subjected to be stolen and then it turns out to be something that the defender has. The examples of this approach includes, token, certificate and smart card.
- Something you are:

  The technique of involving human traits makes the biometric way of authentication to be superior. Moreover finger prints can never be lost at all. Once in a time people felt biometric sensors as very expensive one. But by the advent of smart phones, it reduces the inconvenience involved in buying expensive biometric sensing devices. A typical smart phone that has the biometric sensing is presented in figure 2.

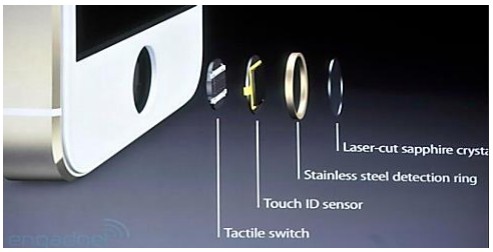


Figure 2.Sensor enabled smart phones

Risky systems and applications deserve a high level authentication scheme that indulges the user, consuming his precious time but fails to identify the user's identity. It is highly necessary to confirm that the person who has entered the application with the username is the person whom he or she claims to be. This sort of high level authentication can only be exhibited by embedding high level and advanced authentication framework in the system or applications. Also it could be risky if malpractice is performed on it.

It is highly essential to maintain security of the application framework by means of a stronger authentication framework. And the modern smartphones that are available in markets have the property to scan and sense the finger-print of the users. Previously sophisticated systems had the ability to sense the finger impressions. But as improvised technology has ruled its way, the finger-print sensors are now available in smartphones itself.

The authentication schemes adopted for user authentication have to be given prime importance.

### 1.1.1. Knowledge based authentication

This technique demands the user to reply for a question which is not known to others. This question remains to be secret. The scheme adopted for password based authentication is the most familiar form of authentication procedure widely in use. But there are several flaws in using this scheme as it uses a text to be remembered to gain access into the system. As the text could be possibly guessed by any unauthorized user to break into the system, the notion of using encrypted password came into practice. The idea behind using the encryption technique is that, the password alone is encrypted and decrypted. But still there exist drawbacks in the system as the passwords can be easily guessed out and even if the passwords are encrypted, they can be easily crack opened.

Moreover using encryption techniques in the system causes a risk of burdening the system. And if the approach of using a long series of passwords, remembering all the password series is difficult which makes the authentication work tiresome and the user may get frustrated, if s/he is not allowed to access his own account. As the passwords are usually stored in the servers, the eavesdropping attack

on the servers can easily precede for obtaining someone's password. On the whole, the fact that makes the password based authentication a failure is that, the servers store the passwords and the servers are viable of being attacked, thus making the scheme unsafe. [2, 3]. They are expressed as attacks which are,

- Wire sniffing
- Man-in-the-middle attack
- Replay attack
- Hash injection
- Trojan
- Password guessing
- Phishing attack
- Pre-computed hashes
- Rainbow attack

### 1.1.2. Token based authentication

The example of token based authentication involves the technique adopted in cryptographic methods. Public key cryptography is a technique where keys are used for authentication process. The keys involved in this process are the private and public keys. Both these keys are mathematically associated with each other. The private key is usually used as the key which is to be kept as a secret one, and this is the key involves in the decryption process, whereas, the public key is associated with the process of encrypting the messages that are sent and received between the clients. The public key also does the process of signature verification together with encryption. Publishing of public keys online is the main benefit that stays behind the public key cryptography thus making the key accessible to all the users in an easy way. It involves the transfer of symmetrical encryption, a computational technique to encrypt the messages by means of fast embedding algorithms that are very simple. The drawback of this technique is that, the computational techniques adopted for these schemes are usually complex [4].

### 1.1.3. Biometric based authentication

Biometric technique that involve in the authentication process, finds itself best in the process of authentications that are so far used. Biometric authentication is found to be very useful in several organizations for gaining access over devices like, ATM machines, desktop computers, and also systems that manage the control of safety doors. The systems that adopt biometric authentication identify persons, depending upon their physical traits like fingerprint impression, facial features, iris recognition, etc. The system not only adopts physical features but also adopts behavioural features like signature, typing rhythm, speaking style etc. As such features are linked to a specific user through physical means; such an authentication is natural and more effective for confirming the access of users who are authorized into the system. The application of biometric authentication is instigated in passports and voter IDs, thereby leading to an advanced secured system. The biological traits utilized in this system offer various authentication outcomes [5, 6]. The pros of using biometrics are,

- Personal data are never used in biometrics, so they cannot be stolen.
- Biometrics is used instead of passwords and ATM card numbers that can be stolen.

Biometric authentication can thus be classified based on physical features and human behavioural characteristics as in figures 3 and 4.

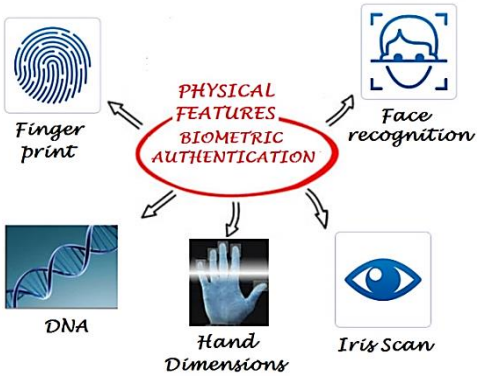


Figure 3.Physical features for biometrics


Figure 4.Behavioural features for biometrics

As already mentioned above, the research work is performed on the usage of smartphones that have biometric sensing

feature of finger-printing trait. Finger-print is believed to be more secure when compared to the iris, as eye donations are possible. Even though fingers of the dead man can be cut or cloned impressions of the fingers can be made by the unauthorized intruders to break open into the systems, the world moving towards drastic innovations has triggered the feature of sensing the difference between the finger of a dead man and the living one.

The real time example of involving the fingerprint trait is being experienced throughout India, as the government has started an initiative to stop the activities of the people who actually being fake, masquerade themselves as valid mobile subscribers. The scheme goes as, "Aadhar-based eKYC", where all the mobile users must link their aadhar ID with their mobile number [7].

### 1.2. Presence service

The mobile device that uses OSNs involves presence service, a service applied in every application of online social media. It is nothing but displaying the details about the users who have entered the application for chat which is one of the core actions that a good social networking application should possess. The details displayed about the person who have arrived into the application are exhibited by algorithms that are designed to search these data. Such data are generally coined as "buddy info" [8].

When the circumstance comes to social network applications, there is a need of buddy info to be transmitted to all the users who are currently available in the network. These messages that are to be transmitted just to broadcast the friend-list information pave way for heavy load to the server. A better way of authentication is needed for any OSN framework incorporating this issue. So, it is very necessary that the application ought to be built upon reliable, scalable, and efficiently distributed server architecture.

The load balancing problem occurs in the server side when there are many clients approaching the server for the service that the server provides. As for OSN applications, the problem of scalability is a major issue. When there is more number of clients approaching the server, the server automatically feels it burdensome to provide its support mutually to all the clients. The server's main function is to provide efficient service distributed equally to all the clients adhered to its network with no compensation in its performance. If the server provides better functionality to some of the nodes adhered to its network and it fails to provide better functionality to other nodes of its network, then such a server gains a pitfall as it has lost the main features that a server must possess like availability, reliability, scalability, response time, latency time, turn-around time, improved performance, load balancing, data consistency, fault-tolerance, etc. [9].

There are various researches conducted on OSN that are of decentralized ones. Safebook is a decentralized online social network which is aimed to the purpose of safeguarding the private information about the user's details. It comprises the feature of finding out the activities involved in mishandling the actions, which could possibly affect the services offered by OSNs. It is also framed to uncover the possible attacks externally by means of eavesdropping or modifying the data present in the networking layer. The Safebook is framed to differentiate the participants and the non-participants of OSNs. This is done with the help of the overlay architecture embedded with the Safebook termed as matryoshka. This overlay architecture is designed to reject unauthorized request, conceal the availability of the users, and also enhance the availability of users' profile. All the functions mentioned are performed by means of replication [10].

To locate the users of OSNs, it uses a peer-to-peer substrate. Here the response time is more important where researchers make use of a peer-to-peer structure called Kademlia to gain a rapid search on the users of OSN.

Tribler is primarily a P2P content sharing system that controls the relationship and tastes of the clients who are logged into the system to swiftly find out the preferences of the digital contents which the users required from online social media. The main objective of this technology is to support the users with end-to-end streaming content based P2P technologies like client computers. Tribler suggests friend recommendations regarding the clients of OSNs to other users of OSNs, holding a condition that they have the same preferences. To ensure the privacy of group formation among the clients of Tribler at the time of registration, each client is provided with an email which is protected, identical and a permanent one. The permanent identifier thus

provided can be also obtained from social networks like MSN and Gmail. The Tribler has mega-caches present within its peers. These mega-caches hold diverse information relevant to friend-list, friend preferences etc. [11].

The disadvantage of the Safebook and Tribler OSN is the authentication procedure, which involves the cryptography technique. In this system, when the user who has already registered into this application makes a revisit to this application for the second time, he or she is involved with the activity of transferring more number of keys. If the user avoids the transfer of more number of keys which is tedious, the user has to assume as a new identifier to OSN, which could disappoints an already existing user. Remembering the passwords is also very complex.

FOAF is another technology towards the decentralized OSNs. Here the framework involves trusted server that allows the clients to store their profiles in them. This technique finds itself advantageous in a way that, it is compatible to the OSN platforms and a full-fledged web-based approach. Though the profiles are stored in the trusted servers, issues related to security still exist [12].

The chief essential features of OSNs are data storage and interaction, which is the major characteristic feature of peer-to-peer systems. These two features are efficaciously applied as file sharing and Instant Messaging (IM) [13, 14] in the case of jabber, or telephony in the case of Skype [15]. The storage feature of these systems may subject the system to a bottle-neck problem as the number of users gets increased.

## 2. PROPOSED SCHEME

The logic behind social media leads to the progress of OSNs, making the user details visible only for the users who have logged into the application. The innovation in proposed work head towards both the server-side and client-side to a more secured framework called RAEF, which connects both these ends to support a reliable architectural framework. RAEF encompasses the action of server-side for better friends' search by minimizing load and for addressing scalability problem, and the action of the client-side for a better authentication procedure.

The main objectives of the proposed system are,

- Reduce server load
- Manage many number of clients
- Update the friend-list frequently
- Exchange instant messages
- Provide a secured chat

### 2.1. RAEF architectural framework

In architectural perspective, the server side includes the over-lay architecture and in the client-side, the authentication process occurs. Thus, the main benefit of Frenzie app is that, the server-side enables faster friend-list search thereby avoiding the single server load to do so, and the client-side finds authenticated chat. When both the server and the client sides follow a stout notion, it makes the frenzy cloud application framework more reliable [16]. The RAEF architectural framework is exhibited in figure 5.

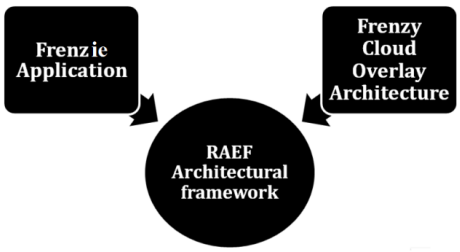


Figure 5.RAEF Architectural framework

### 2.2. Frenzie application

Frenzie is a social network application framed in the research so that it can be installed in the smartphones for instant chat. The facility of smartphone to sense and scan finger prints is used in this research.

The procedure that is adopted for authentication in Frenzie application is provided in figure 6.

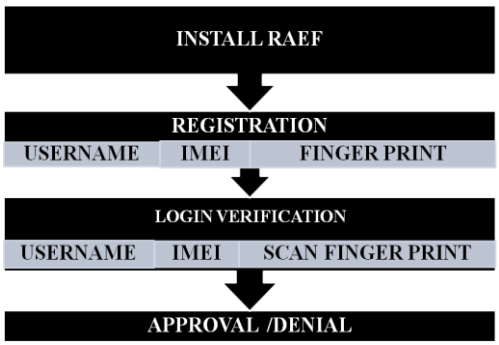


Figure 6.Authentication process involved in Frenzie application

The user installs the Frenzie app first and registers with the username and undergoes fingerprint impression with the aid of the smartphone's fingerprint scanning device. The

fingerprint scanner scans the fingerprint of the user and stores it in database which is distributed to the servers of the Frenzy Cloud overlay. As he submits these two details, the system automatically gets the IMEI number associated with his SIM.

As stated above, along with the biometric, the IMEI number of the mobile user is also taken into account for authentication. If the user re-owns a new IMEI number later, then that number is registered into his or her account in the Frenzie application within the Frenzy Cloud framework. This idea is followed because, in online social media, there is a greater chance of any user to steal the identity of another person and masquerade himself as that person, and chat to make the original person lose his reputation in the society. Criminals usually post messages in the name of popular figures to spoil their name and fame. To control this mischievous activity, Frenzie application has involved in a process of authentication that uses the user's IMEI number to be involved in authenticating the users to the social network. In case of any such malpractice, the culprit could be quickly traced out by the IMEI number, which will reveal the location of the user and the user could be caught easily. But this is not the case in computer system, because there are chances to create fake IP addresses. But as with mobile phones, as IMEI number is a universal number, it helps in tracing the misuser effectively.

The code involved for finding the IMEI number is given below.

```
android.telephony.telephonyManager.getDeviceId()
```

The above code is merely responsible to get IMEI number from smart phones. To get the privilege, it is a must to have the following package and the code.

AndroidManifest.xml:

```
< uses − permission android: name =
"android.permission.READ_PHONE_STATE"/>
```

### 2.3. Frenzy cloud overlay for Frenzie application

Overlay framework is used in this technique where the servers are arranged in a cloud as a distributed network [17]. The cloud thus framed to form an overlay called as the frenzy cloud. As the name exhibits, it is framed with an algorithm that displays the friends' list.

The mobile presence service keeps up the user's existence in the network. It is an important core factor in social network applications. With the help of the mobile presence services, the users who have logged into the network can message instantly with each other. But, to get the presence information about our friends who are currently in the network, there are more number of messages that has to be transmitted between the servers and the clients. These instant messages that the users share with each other, causes the server's load to increase and thereby causes scalability problem to the server when the number of clients who have entered the network increases. To address this issue, an architecture called frenzy cloud is introduced. The Frenzie application which is a secured authentication finds itself compatible with the over-lay framework upon which it is built.

The user logs into the frenzy cloud and occupies the presence server node 'r' then the user issues friends' list search message, F to the presence server node 'r'. On the instance the presence server node 'r' receiving the message F from the user, it searches its registered users and sends its details to the user with one hop strategy.

The overlay architecture of a distributed online-social media is designed in such a way that, the server provides the best service to all the clients who are present in the network irrespective of being placed in a distant location. The proposed system is proved to be successful in balancing the load that the server suffers due to scalability issue. To deal with the scalability and the load balancing issue, over-lay architecture is used. It has a cloud comprising of many servers in a grid quorum fashion following one-hop strategy. After the client registration inside the Frenzie application, the client is directed to any one of the grid IDs 1,2,3,4,5,6,7,8 and 9 by the use of SHA algorithm so that the load usually occurring in the server-side is managed effectively. The servers are actually arranged in the grids from 1 to 9 in the form of rows and columns to exhibit one hop strategy easily.

#### 2.3.1. One-hop caching

The friends' list is available in the server nodes. As the user leaves or enters the server node, the server to which the user is

attached performs the friends' searches that are present in other grid servers within the range of one hop inside the grid of the frenzy cloud. Since the hop is one hop, the neighbouring servers replicate the friends list at every instance thereby updating the friends' list, when the user enters or leaves the Frenzie application.

The search and cache of friend-list within one hop is exhibited in figures 7 and 8 respectively. Say for example, the user is allocated to the presence server having grid ID 4 in the frenzy cloud overlay. When the node in the grid ID 4 has no more users in it, it replicates the friend-list data to other grid IDs (other presence servers within the cloud).

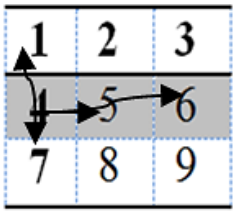


Figure 7.Friends list search

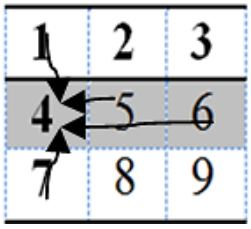


Figure 8.Friends list cache

### 2.3.2. Updating the buddy list

The user when leaves the presence server node (server), i.e. when the user logs out from the application, that particular user's ID (name) is removed totally from all the presence servers and so this particular name is not visible in the Frenzie application too. Therefore the other users in the buddy list can no longer chat with the user. This is the working structure of over-lay architecture upon which the RAEF framework is actually built.

The privacy of the chat is a basic necessity when it comes to social networking. It never allows a third party to enter our chat. In the proposed Frenzie application, the friends of our circle gain approval before the chat, and make our chat to be smooth driven, which is the most desirable in any online social network. The proposed system RAEF incorporates features to support both the server and the client sides, which are its two destinations. RAEF's enhanced support has paved a way for a better online social network application.

Thus, the proposed work is intended to address two major issues that occur in all common online social network applications such as authentication that is incident on the client-side and scalability problems that is on the server-side.

## 3. RESULTS AND DISCUSSION

The user installs the Frenzie application into the smartphone. The homepage of the Frenzie application is shown as presented in figure 9.


Figure 9.Home page


Figure 10.Frenzie registration page

Figure 10 shows the registration page of Frenzie application. The user provides his/her name and provides the fingerprint into the scanning part of the mobile; the fingerprint scanning is shown in figure 11. The next figure 12 shows that the user has entered his name and has successfully registered.

Figure 11.Fingerprint scanning


Figure 12.User successfully registered


Figure 13.Frenzie user login through fingerprint scanning

After successfully registering into the application, the user goes back to the main page and login into the system by placing his finger on the scanning part of the mobile. This is shown in figure 13. This leads to a verification process where finger is processed for scanning and the user is identified. This is shown in figure 14 that the user is accepted.


Figure 14.Finger-print verification-user accepted

If the user is not identified then the scenario will be as depicted in figure 15.


Figure 15.Fingerprint verification-user denied

Regarding the server-side issues that the over-lay architecture undertakes in handling the number of friends for solving the scalability and the load problems, when compared to other presence architectures like mesh-based and chord based [18], the frenzy cloud ensures to be having the best latency time. This is given in figure 16.

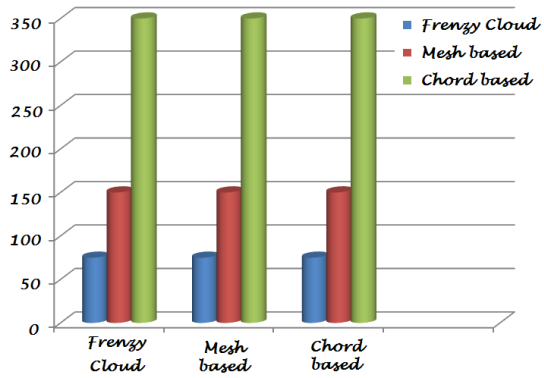


Figure 16.Presence service techniques - a comparison

## 4. CONCLUSION AND FUTURE ENHANCEMENT

The over-lay architecture is designed so as to enhance the functionality that the server has to abide with; the next focus is on the application's authentication that provides integrity by matching the correct user with the correct identifier (fingerprint) that he/she has registered at the time of registration in the application. Such a secured application is named under 'Frenzie' that involves a better way for authenticating the user. Here the users are registered and authenticated with their biometric trait. With the help of the finger-based authentication technique, the users are initially registered with their finger-prints

along with their username. The finger-prints are stored in the servers that are found to be distributed in the frenzy cloud overlay architecture. Automatically the IMEI number associated with the user is registered. The finger-based authentication is found to be a better choice in 'Frenzie' because, the mobile accepts only the registered user finger to gain access on application. This scenario clearly depicts the way in which the finger-based authentication is very secure than the other authentication schemes, where all the other authentication schemes just require the username and password to break into other user profiles without the knowledge of owner of that profile, whereas, Frenzie needs the physical action of the user, in which his or her finger is to be given for matching his identity stored in the database of the server. Thus the over-lay architecture and the 'Frenzie' application make the communication in the OSN to be highly reliable, scalable and an effective one.

Data encryption has to be further focussed. This process of applying encryption and decryption procedure could still secure the messages to a great extent. Base 64 encoding schemes are usually adopted, but it is suggested to use more efficient ones for such a purpose.

## REFERENCES


[1] Tiance Dong, Chenxi Liang and Xu He, Social Media and Internet Public Events, Telematics and Informatics, Vol. 34, No. 3, 2017, pp. 726-739, https://doi.org/10.1016/j.tele.2016.05.024.

[2] S.Chiasson, E.Stobert and A.Forget, Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, 2012, pp. 222-235, http://dx.doi.org/10.1109/TDSC.2011.55.

[3] S.Umamaheswaran, K.Senthil and R.Rajaram, An Algorithm for Encrypting/Decrypting Textual Messages, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 1, 2015, pp. 1-10, http://dx.doi.org/10.18831/djcse.in/2015011001.

[4] P.Tanvi, G.Sonal and S.M.Kumar, Token Based Authentication using Mobile Phone, Communication Systems and Network Technologies, IEEE International Conference, India, 2011, http://dx.doi.org/10.1109/CSNT.2011.24.

[5] C.Berin Jones, Cyber-Security and Combatting Cyber-Attacks: A Study, Journal of Excellence in Computer Science and Engineering, Vol. 3, No. 2, 2017, pp. 1-16, https://dx.doi.org/10.18831/djcse.in/2017021001.

[6] C.T.Li and M.S.Hwang, An Efficient Biometrics-Based Remote User Authentication Scheme using Smart Cards, Journal of Network and Computer Applications, Vol. 33, No. 1, 2010, pp. 1-5, https://doi.org/10.1016/j.jnca.2009.08.001.

[7] http://pmjandhanyojana.co.in/link-aadhar-card-mobile-number/.

[8] Karin Weber, Beverley Sparks and Cathy H.C. Hsu, The Effects of Acculturation, Social Distinctiveness, and Social Presence in a Service Failure Situation, International Journal of Hospitality Management, Vol. 56, 2016, pp. 44-55, https://doi.org/10.1016/j.ijhm.2016.04.008.

[9] Y.Vidya and B.Shemimol, Secured Friending in Proximity Based Mobile Social Network, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 2, 2015, pp. 1-10, http://dx.doi.org/10.18831/djcse.in/2015021001.

[10] L.A.Cutillo, R.Molva and T.Strufe, Safebook: A Privacy - Preserving Online Social Network Leveraging on Real - Life Trust, IEEE Communications Magazine, Vol. 47, No. 12, 2009, http://dx.doi.org/10.1109/MCOM.2009.5350374.

[11] J.A.Pouwelse, P.Garbacki and J.Wang, TRIBLER: A Social-Based Peer-to-Peer System, Concurrency and Computation: Practice and Experience, Vol. 20, No. 2, 2008, pp. 127-138, http://dx.doi.org/10.1002/cpe.1189.

[12] J.Golbeck and M.Rothstein, Linking Social Networks on the Web with FOAF: A Semantic Web Case Study, AAAI, Vol. 8, 2008.

[13] Sara H.Hsieh and Timmy H.Tseng, Playfulness in Mobile Instant Messaging: Examining the Influence of Emoticons and Text Messaging on Social Interaction, Computers in Human Behavior, Vol. 69, 2017, pp. 405-414, https://doi.org/10.1016/j.chb.2016.12.052.

[14] Cosimo Anglano, Massimo Canonico and Marco Guazzone, Forensic Analysis of the Chat Secure Instant Messaging Application on Android Smartphones, Digital Investigation, Vol. 19, 2016, pp. 44-59, https://doi.org/10.1016/j.diin.2016.10.001.

[15] Paul Hanna, Using Internet Technologies (Such as Skype) as a Research Medium: A Research Note, Qualitative Research, Vol. 12, No. 2, 2012, pp. 239-242.

[16] M.Julie Emerald Jiju and E.Arun, Cloud Computing: Characteristics, Issues and Possible Security Solutions - A Review, Vol. 1, No. 2, 2015, pp. 12-23, http://dx.doi.org/10.18831/djece.org/2015021002.

[17] V.G.Gopika and Neetha Alex, A Secure Steganographic Method for Efficient Data Sharing in Public Clouds, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 2, 2015, pp. 11-22, http://dx.doi.org/10.18831/djcse.in/2015021002.

[18] Chi-Jen Wu, Jan-Ming Ho and Ming-Syan Chen, A Scalable Server Architecture for Mobile Presence Services in Social Network Applications, IEEE Transactions on Mobile Computing, Vol. 12, No. 2, 2013, http://dx.doi.org/10.1109/TMC.2011.263.