

# Three Layer Secure (3-LS) Architecture for Online Social Networks

Mohit Gambhir<sup>1</sup>, Dr. M N Doja<sup>2</sup>, Dr. Moinuddin<sup>3</sup>

**Abstract**— Online Social Network (OSN) is a growing platform which enables people to get hold of news, communicate with family and old friends with whom they have lost contact, to promote a business, to invite to an event of friends and to get people to collaborate. OSNs have suffered from numerous issues like OSNs consume so much of time of the students and working professionals let them create their own worlds. The users often suffer from depression and anxiety because of cyber bullying and privacy issues. Malicious users have found a new method by which their activities can achieve the desired objectives. Many of the OSNs have suffered from lawsuits of unauthorized access of information and sharing of the same. This paper proposes a novel 3- Layer Secure architecture for OSN. This architecture deals with unique global id. for accessing various services on online social world . According to the actions performed by the user on the social world, a trust factor of the user is calculated which is its reputation in the online social world

**Index Terms**— Social media, Online Social Networks (OSN), OpenID, Single Sign On (SSO), Trust Factor, Security, Credibility.

## 1 INTRODUCTION

WITH the development of Web 2.0, the interactive web has become the most popular media today. It has even surpassed the print media and conventional marketing media. The new age is of digital and social media. The Online Social Network (OSN) [1], [2] is a growing platform which enables people to get hold of news, communicate with family and old friends with whom they have lost contact, to promote a business, to invite to an event of friends and to get people to collaborate.

OSN sites are web-based services that allow individuals to (a) create a public or semi-public profile, (b) manage a list of other users with whom they share a connection, and (c) interact with their friends and make new connections. OSNs have also suffered from numerous issues since their beginning two decades before. OSNs have been the centre of attention of being the trend makers which often die as fast as they grow. In this paper, author presents a novel three layer secure architecture is proposed by keeping in mind various issues of OSNs.

Organization of the paper is as follows: section 2 discusses about various issues associated with OSN. A three layer secure architecture is proposed in section 3. This section explains various components of proposed architecture. Last section concludes the paper.

## 2 ONLINE SOCIAL NETWORKS

An OSN is a platform to build social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. An OSN service consists of a representation of each user (often a profile), his/her social links, and a variety of additional attributes. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network. OSNs present the following benefits:

- OSNs provide knowledge to people in almost real time.
- OSNs connect people across boundaries.
- Create an ongoing, shared social space among geographic and departmentally dispersed people [3].
- Keeping in touch with family members that live far away is much easier through the use of OSNs.
- Social networking has gradually evolved as prominent resource/tool for imparting education. It is becoming increasingly important in schools. Facebook, Moodle, SecondLife, Digg, and other sites are often used by teachers to communicate with students or for out-of-classroom discussions [3].

OSNs have suffered from numerous issues since their beginning two decades before. OSNs have been the centre of attention of being the trend makers which often die as fast as they grow. OSNs have always been argued to be affecting the privacy of the users. Apart from this, they have other issues which are outlined as follows:

- With the increasing popularity of OSNs, every other person has an account on at least 3 of the most popular OSNs. OSNs consume enormous amount of time of the students and working professionals.
- The users often suffer from depression and anxiety because of cyber bullying, trolling [4] and privacy issues.

- Mohit Gambhir is currently pursuing Ph.D in Computer Science from Jamia Millia Islamia University, India, Delhi.  
Email:mohitgambhir@gmail.com
- M N Doja is chairman of department of Computer Enggineering, Jamia Millia Islamia, Delhi, India.
- Moinuddin is Pro-VC of Delhi Technological University, Delhi, India,

- Malicious users keep on developing new ways to achieve their objectives.
- Many of the OSNs have suffered from lawsuits of unauthorized access of information and sharing of the same.
- There is no limitation on what an individual can post on OSNs. Thus, there is no way to decide the trustworthiness of a user and the content posted by that particular user. How much can you trust a person and the actions he/she performs on the OSN? There no such model that exists in the current OSNs.
- In OSN credibility of Content and Trustworthiness of user is mere an access control mechanism which covers all the users in the OSNs. And every user has different trustworthiness in different OSN but there is not universal trustworthiness of a user who is further identified by an OpenID.

In this paper, authors proposed a novel three layer secure architecture which could deal with credibility of content and trustworthiness of the user and many other issues of OSN.

### 3 3-LAYER SECURE ARCHITECTURE

3-Layer Secure architecture emphasizes on a mechanism for ensuring safer online world by providing a unique global id for each user, evaluate and compute the Trust factor for a user, thereby measuring the credibility of a user in the OSN space. Need for unique global id (OpenID [5], [6]) is felt so that impersonation is minimized and deeds of a user are tracked in more efficient manner. As of today, Single Sign-On (SSO) [7] is used as one time log in to gain access to all the systems without being prompted to log in again at each of them. Fig. 1 shows the various components of proposed architecture which are divided into three layer viz. Client layer, business logic layer and database layer.

User enters OpenID username and password information on a client computer. This information is forwarded to the OpenID server of Business Logic Layer through Internet Service Provider (ISP). OpenID server checks authentication of user security and forward its request to the corresponding application server in case of successful authentication. Otherwise, block the further processing and generate the error message.

While working on the application server, User's Trust is calculated depending on the actions he/ she perform. The Trust factor considers the actions performed by the user in the OSN and the type of content being posted on the OSN. The posts are divided/ classified into sensitive and non-sensitive category. If a user interacts with the sensitive category posts, the Trust Factor of the user decreases and if the user interacts with non-sensitive category posts, the Trust Factor increases. Trust Factor also depends on the type of posts the user generates in the OSN. The more sensitive posts a user generates, the less will be the Trust Factor.

In this way, the user is held responsible for his reputation in the OSN world. This will enable the users to decide which content is reliable and which user is credible. Cyber bullying, anxiety, depression and other adverse affects of OSN in teenagers shall be easier to curb. It shall become easier to watch that the new generation doesn't indulge in any

malicious activities. This easily directs the Cyber Police to take action to curb the problem before it arises. The relative nature of trust gets abolished and the universal trustworthiness of a user gets materialized.

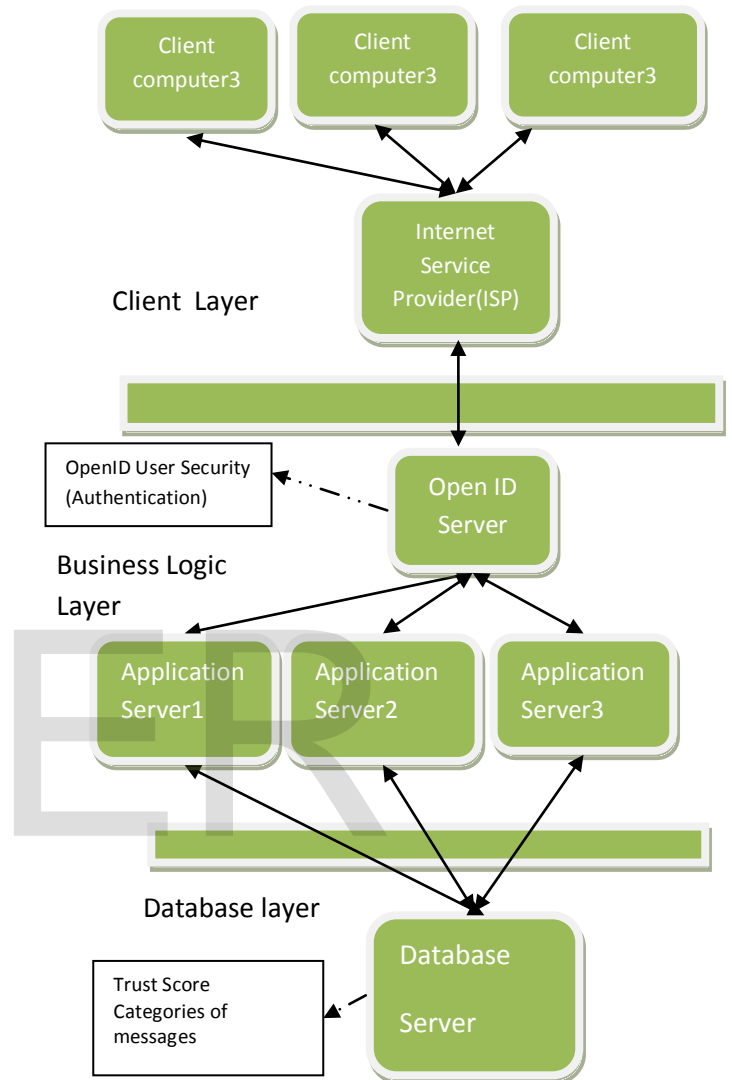


FIG. 1: 3-LAYER SECURE ARCHITECTURE

### 4 CONCLUSION

The proposed architecture removes various issues of OSN by introducing the concept of SSO and calculating the credibility and trust worthiness of the user based on the actions performed by him/ her. SSO enforces user to have single unique id to enter in to online social world. Further, trust is to be associated with that unique id which is said to be its reputation in the OSNs

## REFERENCES

- [1] Laura Garton, Caroline Haythornthwaite, and Barry Wellman. "Studying Online Social Networks." *Journal of Computer-Mediated Communication*, Vol. 3.1, pp. 0-0, 2006.
- [2] Andreas M. Kaplan, and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media," *Business horizons*, Vol. 53(1), pp. 59-68, 2010.
- [3] Nicole B Ellison, "Social network sites: Definition, history, and scholarship." *Journal of Computer-Mediated Communication*, Vol. 13(1), pp. 210-230, 2007.
- [4] Susan Herring, Kirk Job-Sluder, Rebecca Scheckler, and Sasha Barab. "Searching for safety online: Managing" trolling" in a feminist forum." *The Information Society*, Vol 18(5), pp. 371-384, 2002.
- [5] D. Recordon and D. Reed, "OpenID 2.0: A Platform for User Centric Identity Management," in proceedings of the second ACM workshop on Digital identity management (DIM'06). New York, NY, USA: ACM, 2006, pp. 11-16.
- [6] Khan R.H.L, Ylitalo J. and Ahmed A.S., "OpenID Authentication as a Service in OpenStack," in proceedings of Information Assurance and Security (IAS), 2011 7th International Conference, pp.372-377, 2011
- [7] Hyun-kyung Oh and Seung-hun Jin, "The Analysis of SSO in OpenID," in proceedings of APIS, pp.15-18, 2007.

IJSER

# IJSER

WITH the development of Web 2.0, the interactive web has become the most popular media today. It has even surpassed the print media and conventional marketing media. The new age is of digital and social media. The Online Social Network (OSN) [1] [2] is a growing platform which enables people to get hold of news, communicate with family and old friends with whom they have lost contact, to promote a business, to invite to an event of friends and to get people to collaborate.

OSN sites are web-based services that allow individuals to (a) create a public or semi-public profile, (b) manage a list of other users with whom they share a connection, and (c) interact with their friends and make new connections. OSNs have also suffered from numerous issues since their beginning two decades before. OSNs have been the centre of attention of being the trend makers which often die as fast as they grow. In this paper, author presents a novel three layer secure architecture is proposed by keeping in mind various issues of OSNs.

Organization of the paper is as follows: section 2 discusses about various issues associated with OSN. A three layer secure architecture is proposed in section 3. This section explains various components of proposed architecture. Last section concludes the paper.

## 2 ONLINE SOCIAL NETWORKS

An OSN is a platform to build social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. An OSN service consists of a representation of each user (often a profile), his/her social links, and a variety of additional attributes. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network. OSNs present the following benefits:

- OSNs provide knowledge to people in almost real time.
- OSNs connect people across boundaries.
- Create an ongoing, shared social space among geographic and departmentally dispersed people. [3].
- Keeping in touch with family members that live far away is much easier through the use of OSNs.
- Social networking has gradually evolved as prominent resource/tool for imparting education. It is becoming increasingly important in schools. Facebook, Moodle, SecondLife, Digg, and other sites are often used by teachers to communicate with students or for out-of-

classroom discussions [3].

OSNs have suffered from numerous issues since their beginning two decades before. OSNs have been the centre

of attention of being the trend makers which often die as fast as they grow. OSNs have always been argued to be affecting the privacy of the users. Apart from this, they have other issues which are outlined as follows:

- With the increasing popularity of OSNs, every other person has an account on at least 3 of the most popular OSNs. OSNs consume enormous amount of time of the students and working professionals.
- The users often suffer from depression and anxiety because of cyber bullying, trolling [4] and privacy issues.
- Malicious users keep on developing new ways to achieve their objectives.
- Many of the OSNs have suffered from lawsuits of unauthorized access of information and sharing of the same.
- There is no limitation on what an individual can post on OSNs. Thus, there is no way to decide the trustworthiness of a user and the content posted by that particular user. How much can you trust a person and the actions he/she performs on the OSN? There no such model that exists in the current OSNs.
- In OSN credibility of Content and Trustworthiness of user is mere an access control mechanism which covers all the users in the OSNs. And every user has different trustworthiness in different OSN but there is not universal trustworthiness of a user who is further identified by an OpenID.

In this paper, authors proposed a novel three layer secure architecture which could deal with credibility of content and trustworthiness of the user and many other issues of OSN.

## 5 3-LAYER SECURE ARCHITECTURE

3-Layer Secure architecture emphasizes on a mechanism for ensuring safer online world by providing a unique global id for each user, evaluate and compute the Trust factor for a user, thereby measuring the credibility of a user in the OSN space. Need for unique global id (OpenID [5] [6]) is felt so that impersonation is minimized and deeds of a user are tracked in more efficient manner. As of today, Single Sign-On (SSO) [7] is used as one time log in to gain access to all the systems without being prompted to log in again at each of them. Fig. 1 shows the various components of proposed architecture which are divided into three layer viz. Client layer, business logic layer and database layer.

User enters OpenID username and password information on a client computer. This information is forwarded to the OpenID server of Business Logic Layer through Internet Service Provider (ISP). OpenID server checks authentication of user security and forward its request to the corresponding application server in case of successful authentication. Otherwise, block the further processing and generate the error message.

While working on the application server, User's Trust is calculated depending on the actions he/ she perform. The Trust factor considers the actions performed by the user in the OSN and the type of content being posted on the OSN. The posts are divided/ classified into sensitive and non-sensitive category. If a user interacts with the sensitive category posts, the Trust Factor of the user decreases and if the user interacts with non-sensitive category posts, the

- Mohit Gambhir is currently pursuing Ph.D in Computer Science from Jamia Millia Islamia University, India, Delhi.  
Email:mohitgambhir@gmail.com
- M N Doja is chairman of department of Computer Engineering, Jamia Millia Islamia, Delhi, India.
- Moinuddin is Pro-VC of Delhi Technological University, Delhi, India,

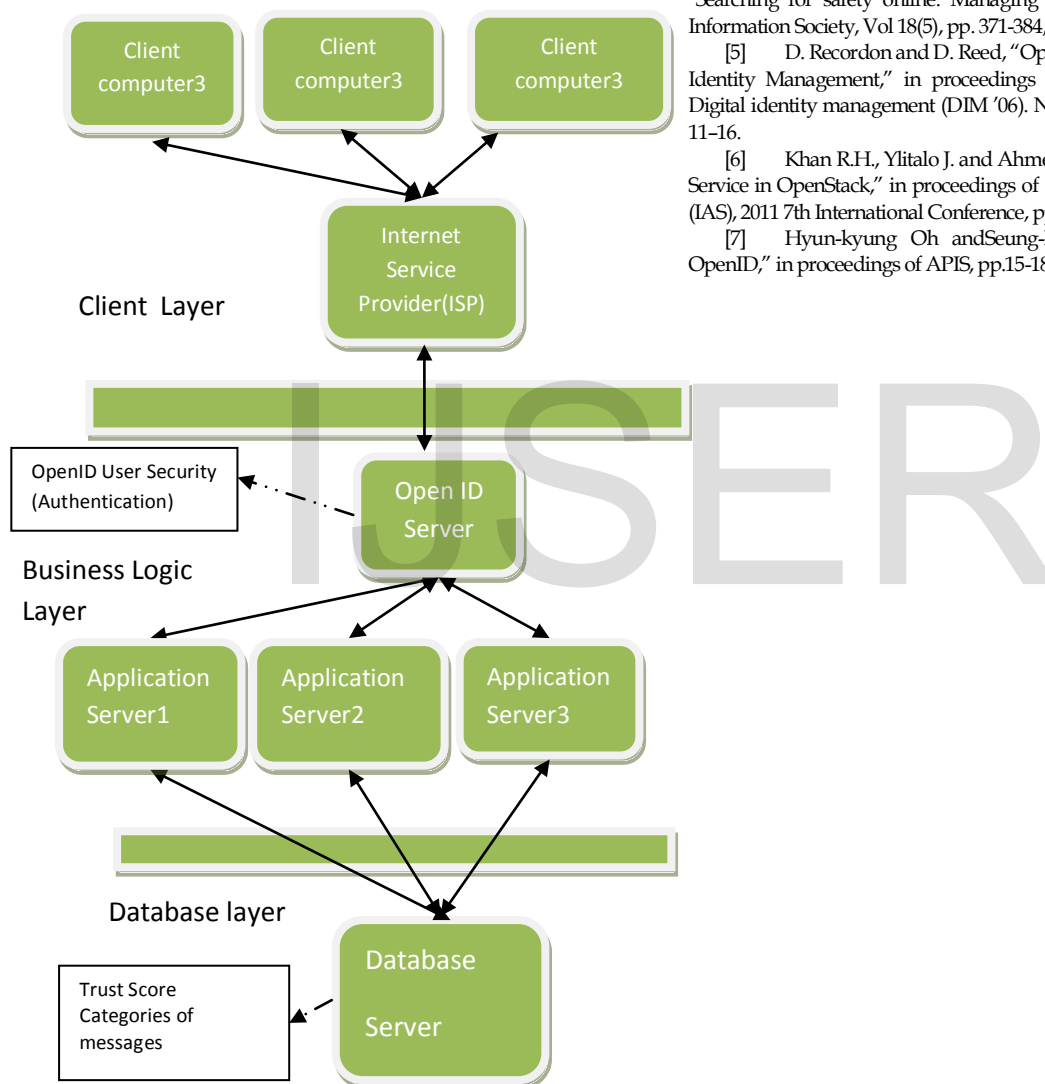
Trust Factor increases. Trust Factor also depends on the type of posts the user generates in the OSN. The more sensitive posts a user generates, the less will be the Trust Factor.

In this way, the user is held responsible for his reputation in the OSN world. This will enable the users to decide which content is reliable and which user is credible. Cyber bullying, anxiety, depression and other adverse affects of OSN in teenagers shall be easier to curb. It shall become easier to watch that the new generation doesn't indulge in any malicious activities. This easily directs the Cyber Police to take action to curb the problem before it arises. The relative nature of trust gets abolished and the universal trustworthiness of a user gets materialized.

actions performed by him/ her. SSO enforces user to have single unique id to enter in to online social world. Further, trust is to be associated with that unique id which is said to be its reputation in the OSNs

**REFERENCES**

[1] Laura Garton, Caroline Haythornthwaite, and Barry Wellman. "Studying Online Social Networks." *Journal of Computer Mediated Communication*, Vol. 3.1, pp. 0-0, 2006.  
 [2] Andreas M. Kaplan, and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media," *Business horizons*, Vol. 53(1), pp. 59-68, 2010.  
 [3] Nicole B Ellison, "Social network sites: Definition, history, and scholarship." *Journal of Computer -Mediated Communication*, Vol3(1), pp. 210-230, 2007.  
 [4] Susan Herring, Kirk Job-Sluder, Rebecca Scheckler, and Sasha Barab. "Searching for safety online: Managing" trolling" in a feminist forum." *The Information Society*, Vol 18(5), pp. 371-384, 2002.  
 [5] D. Recordon and D. Reed, "OpenID 2.0: A Platform for User Centric Identity Management," in proceedings of the second ACM workshop on Digital identity management (DIM '06). New York, NY, USA: ACM, 2006, pp. 11-16.  
 [6] Khan R.H., Ylitalo J. and Ahmed A.S., "OpenID Authentication as a Service in OpenStack," in proceedings of Information Assurance and Security (IAS), 2011 7th International Conference, pp.372-377, 2011  
 [7] Hyun-kyung Oh and Seung-hun Jin, "The Analysis of SSO in OpenID," in proceedings of APIS, pp.15-18, 2007.



**FIG. 1: 3-LAYER SECURE ARCHITECTURE**

**6 CONCLUSION**

The proposed architecture removes various issues of OSN by introducing the concept of SSO and calculating the credibility and trust worthiness of the user based on the