J. Basic. Appl. Sci. Res., 3(12)26-33, 2013

© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A Two Factor Based Anti-Phishing Method in Open ID

Dr. Muhammad Asif[1], Dr. Muhammad Shahzad Sarfraz[2], Mr. Shahbaz Ahmed[3], Dr. N. K. Tripathi[4]

[1]Assistant Professor Department of Computer Science, National Textile University Faisalabad
[2]Department of Computer Science, COMSATS Institute of Information Technology, Abbottabad, Pakistan
[3]Assistant Professor Department of Computer Science, National Textile University Faisalabad
[4]Associate Professor and coordinator at Remote Sensing and Geographical Information System, School of Engineering and Technology, Asian Institute of Technology, PO Box 4, Pathumthani 12120, Thailand

Received: May 10 2013
Accepted: June 23 2013

ABSTRACT

With the exponential growth in web based applications, a typical user has to create a lot of usernames and passwords in order to use these services, while using these services user have to keep track of her credentials which in turns results in high probability of identity theft. A secure and reliable identity management system is required in this scenario. OpenID is a good solution to interact with these services through one identity. However, it is quite vulnerable to different kind of attacks including phishing. To tackle such kinds of attacks, we purpose and evaluate a two factor based anti-phishing method using password and personal identification number which is considered very difficult to break. Proposed protocol works by taking two credentials from the user instead of one i.e. user password and her PIN code for verification at server side. This two factor based protocol is difficult to break even in case a phisher succeeds to get control of the user page.The prototype system is built and tested against the phishing attacks and is found to be strong enough for protection against identity theft.

KEYWORDS: OpenID, Phishing Attacks, Single Sign On, Anti-phishing

I. INTRODUCTION

In recent years with exponential growth in web services, users have to create and maintain lot of usernames and passwords in order to interact with these web sites. Single Signon (SSO) systems is a good way to create one identity and use it for all services. OpenID [1][2][3] is new and emerging light weight protocol for identity management. OpenID 2.0 is a user-centric web single sign-on protocol with over one billion OpenID-enabled user accounts, and tens of thousands of supporting websites [4]. OpenID is a system that enables a user to use a URL as their identification and log into any OpenID-enabled web site using that URL. User doesn’t need to create user IDs and passwords on individual web site. The benefit: As a user of the OpenID system, one doesn’t need to remember the usernames and passwords for individual web site [5].User just needs to create one ID through any of the identity provider server and use it on all relying parties supporting OpenID. There are more than one billion OpenID accounts [23] and a complete list of OpenID enabled sites is available at [24]. However this protocol is quite vulnerable to phishing attacks [6][7][8][10].

Phishing is used to attack digital identities, as phishing can duplicate the same site and is very effective. In past, e-mails were used to lure users to fake websites for the theft of personal information. However, in these days phishing is more complicated and intelligent, and includes malicious codes and Pharming [7]. According to the Anti-phishing Working Group (APWG) [12], the average number of monthly phishing websites in 2007 was 31,160 almost double as compared to those in 2006. The target organizations were based in UK, USA, Australia and Canada. It is estimated that the US lost 3billion dollars as a result of phishing in 2007 [7].It seems that the theories of the globalization stages does not account completely the stages of globalization based on the Internet in a complete and exact way. Because the Internet is a new and direct channel to access target markets and shortens and facilitates the globalization stages for companies. It can be concluded that in the upstream processes international companies show more willingness to use E-commerce[25]. The proposed single sign on based protocol can be embedded in E-commerce websites in order to make them on platform for all.

The main objectives and goals for conducting this research are to overcome the problems associated with the identity theft at web applications. Identity theft causes a loss of billions of dollars as mentioned in previous paragraphs. This research presents a double security protocol system and it works as a safeguard against the identity theft.

The scientific contributions of this research are 1)This research presents a novel method with two factors based authentication mechanism in which a user of the system can get authorization on the system after

[*] **Corresponding Author:** Dr. Muhammad Asif, Assistant Professor Department of Computer Science, National Textile University Faisalabad. Email: asif@ntu.edu.pk

providing its two credentials i.e. username and PIN code. 2) secondly, this improved version of protocol is new in its nature which can be integrated to any kind of OpenID enabled web services.

The rest of the paper is organized as follows, section II gives a brief introduction about the communication in OpenID environment and the parties involved in OpenID communication. Section III describes the existing anti-phishing methods and the problems associated with them. Section IV describes about the proposed anti-phishing method in this research and its usefulness as compared to the existing methods. Section V is about the prototype system description and the integration of proposed system in the prototype system. Comparison of proposed anti-phishing method is briefly described in section VI, this section describes the advantages of using proposed protocol over the existing methods in tabular form and finally section VII gives a conclusion about the current research.

A. Anti-phishing Techniques

Several anti-phishing methods have been proposed and implemented for preventing phishing attacks. The anti-phishing techniques can be classified in two categories namely heuristic-based and list based. Usually list-based techniques maintain white list or a black list of websites. Mostly, anti-pharming mechanisms use a black list to prevent users from accessing phishing sites. Effectiveness of black list filtering techniques mainly depends on different factors e.g., accuracy, freshness and coverage of list of phishing websites. The phishing URL's are normally collected by web crawlers or reported by internet users and list maintainers are generally responsible for verification of listed URL's about their authenticity. A well-controlled and maintained black list can identify most famous phishing sites. However, it cannot obviously filter uncollected, unreported or unanalyzed URL's. It is very difficult for a list to be 100% coverage and up to date freshness [8].

Universal Resource Locator (URL).A phisher may attempt to mislead users by including the @sign in a website URL. User agents i.e. browsers usually treat the text before the @ symbol as the name used to access a website. Users can be redirected towards a fake web resource by using this URL method, for example using URL like www.example.com@ 203.159.10.194. The user thinks he/she is visiting www.example. com, but she is actually being redirected to another site with the IP address 203.159.10.194. Thus, it is important to check whether a URL contains special symbols in order to avoid possible phishing attacks [8].

Domain name. A phishing site can register a domain name similar to the target site. For example, paypa1.com andpaypal.com look the same, but the first one is actually paypa plus the numeral one. Distance between two strings can be measured by applying several metrics e.g.[9] distance. The measured distances can be used as an index to identify possible phishing sites.

In section II we discuss normal flow of communication in OpenID environment and the scenario where OpenID is vulnerable to phishing attacks. Section III describes the related techniques used to address the phishing attacks. We discuss proposed protocol and demonstrate a prototype system for protocol strength in section IV and V. Section VI gives a comparison table between proposed and existing anti-phishing methods. We conclude the discussion in section VII.

II. Communication in OpenID

OpenID is a decentralized mechanism of identity management for SSO. It works on a set of communication protocols, and different parties communicate with each other in order to authenticate a user. There are three major components in any OpenID system: Relying Party (RP), Identity Provider Server (IdP), and User Agent. These components interact with each other during the authentication process [5]. Roles for these components are explained below.

Relying Party (RP) is normally a web resource including website or some web services, a user wants to interact by providing his/her OpenID. On receiving this Id RP initiates a service discovery through Yadis [21] protocol for discovering the Identity Provider server. An association handle is created between the RP and the IdP for information exchange in the later part of authentication and is shown in step 2 of Figure1. Once the IdP is discovered and the association handle is created the RP redirects the user agent towards server for authentication.

The Identity Provider (IdP)is the OpenID provider server that holds an End User's credentials. The Identity Provider will validate the ownership of an identity. Usually it can exchange the protocol messages with RP for information exchange. An IdP is capable of issuing an id, usually in the form of a URI e.g. "asifait.pip.verisignlabs.com" is an example of an OpenID issued by a central IdP server from VeriSign Identity Protection. In step 4 of Figure1 the user is authenticated by the IdP by his username and password. After user authentication the user browser is redirected towards the RP and now the user can use services of RP as an authenticated user.

User agentis the end user’s browser who wants to communicate with the OpenID enabled services. In step 1 of Figure1 the user initiates a session with the RP by providing his/her Id and then the rest of the steps occur. Figure1 below shows a set of communication among these parties.

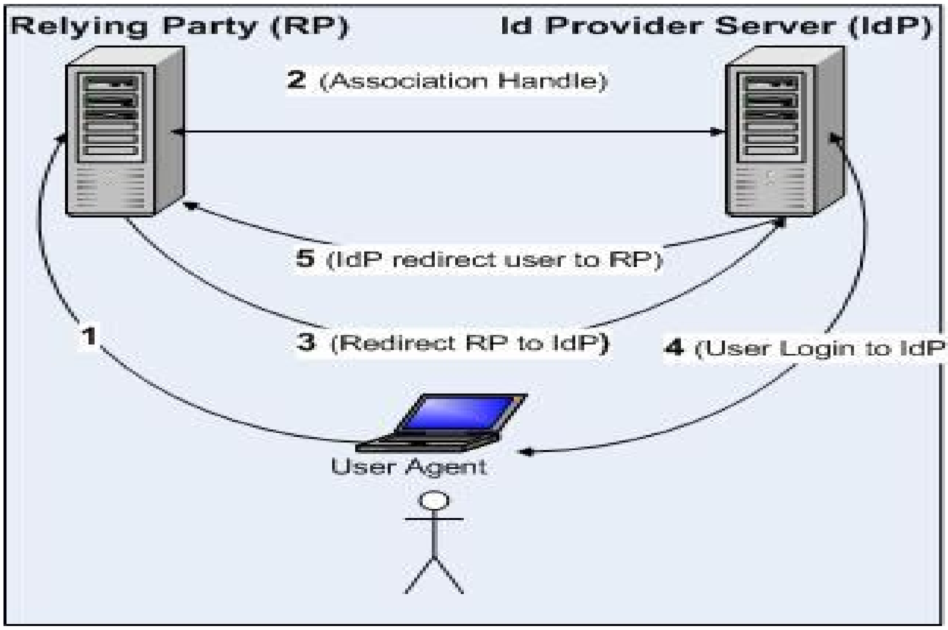


Figure-1: Communication in OpenID components

A. Vulnerability of Phishing Attack in OpenID

Phishing is a malicious activity where an attacker (phisher) tries to trick Internet users in providing confidential information [13]. Phishing is a serious problem in web based applications because with phishing intruder can steal sensitive information like bank account details, social security number and credit card number [8]. OpenID is a light weight and easy to implement protocol for SSO systems but it is vulnerable to phishing attacks [7][8][10][11]. Figure2 shows a scenario of phishing attack in OpenID communication. When a user agent provides his id to RP for using its services, then malicious RP can redirect the client browser to a fake server designed similar in look and feel of original server as shown in step3 of Figure2. The user thinks he is on original server and provides his credentials to the server and this is the point of Phishing in OpenID.

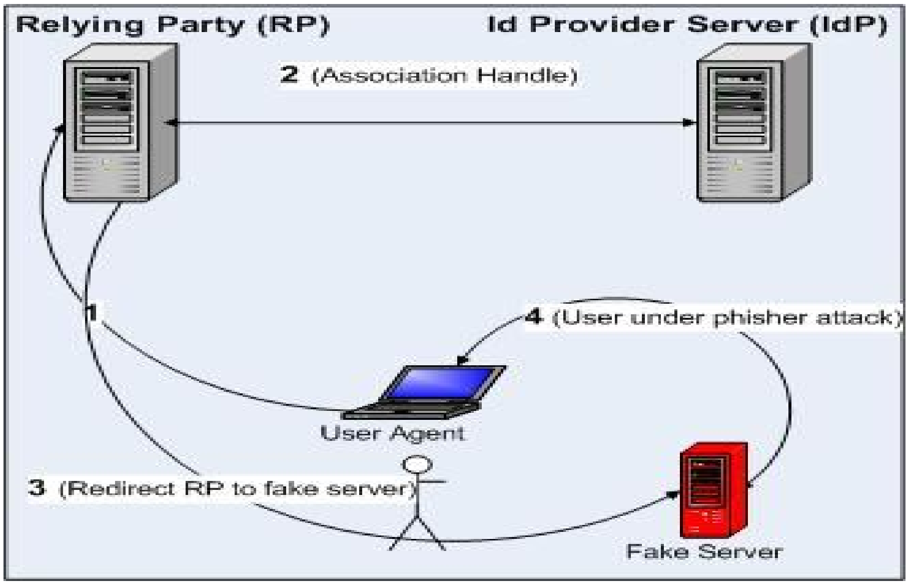


Figure-2: Phishing scenario in OpenID communication

III. Related Work

Single sign-on (SSO) is mechanism where a single user action for user authentication and authorization can allow a user to access all services, computers and systems, where he has access permission, without the need to enter multiple passwords [14]. SSO consists of different kind of architectures, some of them deal with a single set of credentials and the some are deal with multiple credentials. The former are normally PKI-based and token-based systems. The cookie-based and Kerberos-based are both the token-based SSO systems. For the latter, there are credential synchronization-based system, secure client-side credential caching system and secure server-side credential caching system [15]. Since OpenID is cookie-based systems, so we discuss only authentication process of cookie-based systems. Here we discuss some of the existing anti-phishing methods.

A. Existing Anti-Phishing Methods

Some anti-phishing methods for OpenID have been presented, for example my OpenID’s Personal icon[12];VeriSign and IE7's Extended Validation Certificate[16, 17];VeriSign and Firefox's seatbelt[17, 18]; Vidoop’s new password solution[19] and Jabber's authentication by a messenger or SMS[20]. My OpenID’s Personal icon: Personal Icon works just like Yahoo's Sign-in Seal. Because an OpenID provider (OP) has a cookie for a user's PC, an OP redirected by an RP shows pictures or texts initially input by the user. VeriSign and IE7's Extended Validation Certificate: This was jointly developed by VeriSign and IE7.If an OP is an OP verified by VeriSign, a web browser's address window turns Green. This certificate is available only for IE7 and costs about $1,000.VeriSign and Firefox's seatbelt: This was jointly developed by VeriSign and Firefox. If an OP's address is different from one previously set, seatbelt shows a warning message. Like Personal Icon; it can be used only on the user's PC and not on other PCs. Vidoop's new password solution: When a user signs in with Vidoop, a picture is selected instead of a password. An activation code is issued by e-mail and a picture is used as an input for password. Jabber's authentication by a messenger or SMS: If an RPis redirected to a correct OP, the OP lets a user know this by a messenger or SMS. To use this, a user should log in to a messenger or have a device with which to receive an SMS message.

IV. Proposed Anti-phishing Method

In this paper we propose and evaluate a new method based on two factors i.e. password and Personal Identification Number (PIN). It was found that the proposed model have the capacity to make it very difficult for intruders to phish the RP. This model works as follows:

During initial registration on any IdP, user have to give their personal information including name, address, phone no. etc. that is stored on the IdP for user verification and this information might be used by some of the RP in order to facilitate user for more services at RP. In this model we have proposed and implemented another factor in protocol message called PIN, a four digit numeric code like an Automatic Teller Machine (ATM) code. We store this PIN code at the server side in encrypted form e.g., md5 encryption. Now let’s discuss about user authentication on this kind of server, during Step1 of user authentication, id is provided to the RP along with his PIN code. In Step2 of the Figure3 the RP creates a association handle with the IdP and redirects the user towards IdP in Step 3 and now in Step4 the IdP authenticate the user by his username and password. If the user is successfully authenticated, IdP sends a success message to RP along with the stored PIN of this user as shown in Step5 of Figure3. In this model at RP side we get the encrypted PIN from the server and compare the two PINS e.g., one provided by user to RP and the other returned from the server, if the operation is successful, RP give access to the user for using its services otherwise it rejects the user.

Now consider a situation of phishing which is discussed above. Let’s imagine after Step1 inFigure2, an intruder comes in this situation and redirects the user browser to some fake server with a phishing attack, in this situation the user is under attack as in Step 3 of Figure2. Because this server is fake and having no information on user PIN code, in this case it will be impossible for intruder to guess and return the user PIN code to RP and once the RP does not receive the correct encrypted PIN code from original server, RP computation method will not allow user to authenticate its services to user. This scheme shows the protection against phishing by using a second factor PIN which is only stored and accessed through original IdP server, even though the user agent is phished to some fake server they cannot get the PIN code from this server. The schematic diagram of this model is shown in Figure3. In section V we demonstrate this model through a prototype system.

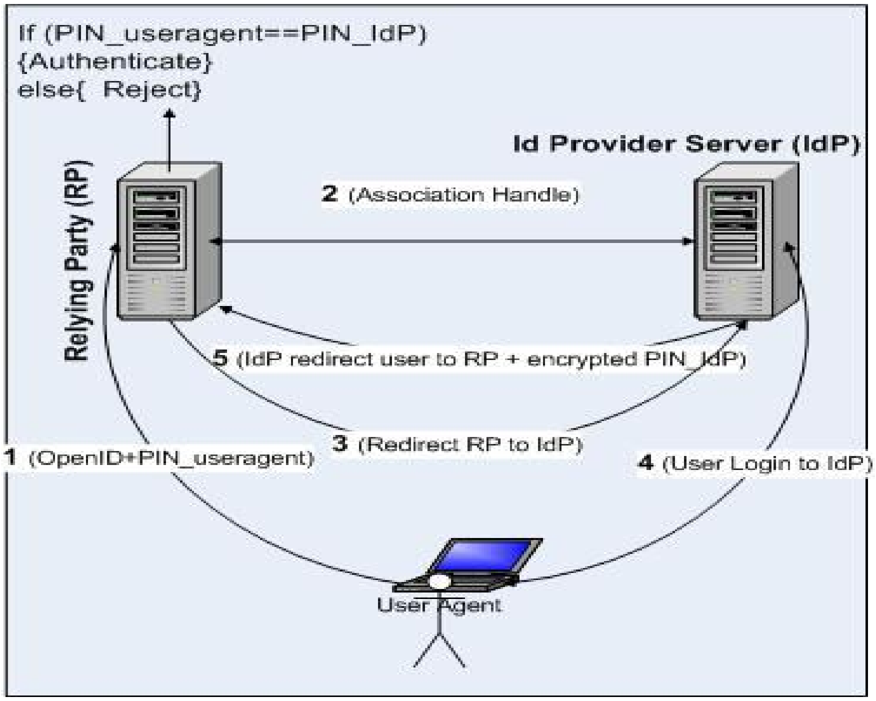
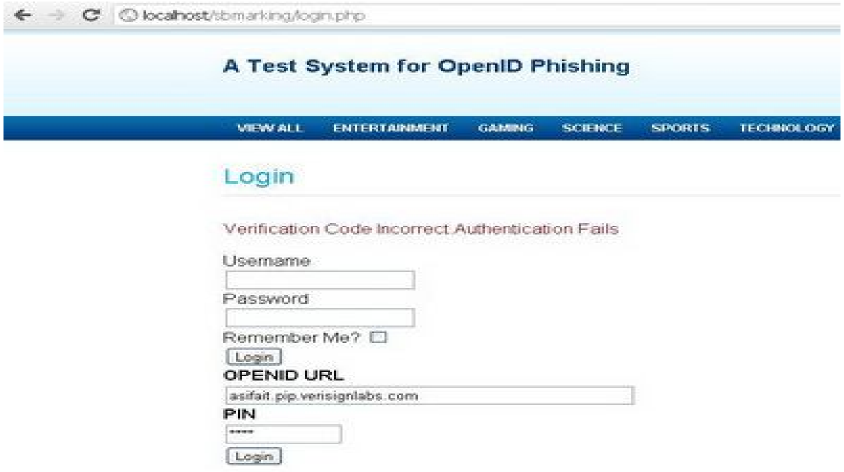


Figure-3: user authentication scenario using proposed model

V. Prototype System Description

We have tested the proposed model of anti-phishing by developing a prototype system, a social book marking and tagging application as shown in Figure4. The prototype system has two ways of authentication for the user: one is the normal authentication through conventional username/password and the other is through OpenID URL. This system gets the OpenID of user along with his/her PIN code as shown in Figure 4. In the second step this RP redirects the user browser towards the IdP through its discovery protocol using Yadis [21] and the IdP server authenticate the user first by exchanging username/password with user and then exchange a protocol message with RP by sending encrypted PIN code. If the user does not enter correct PIN code at RP or RP does not receive the correct PIN from IdP, it will never allow user authentication. In Figure 4we entered a wrong code and got error message. In this way if there is a phishing attack on our proposed RP, the intruder, in result might steal the user credentials like username and password but they cannot have access to user PIN which is stored at IdP and hence cannot be authenticated by the RP which implements this second factor. Figure5 shows a data exchange message between our RP and the IdP server, for this prototype system we have used the pip VeriSign labs OpenID provider server[22]. This data exchange includes the data that is being transferred from OpenID provider server towards the RP.



Verification Code Incorrect.Authentication Fails

Username

Password

Remember Me? □

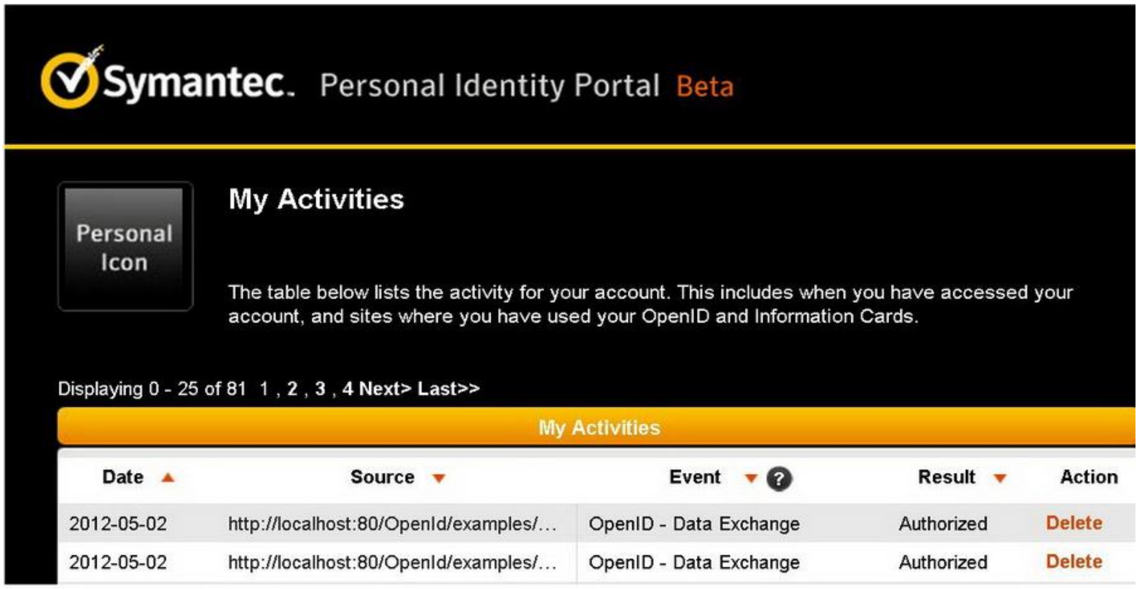
OPENID URL

asifait.pip.verisignlabs.com

PIN

****

Figure-4: user authentication scenario in prototype system using proposed model



Symantec. Personal Identity Portal Beta

My Activities

The table below lists the activity for your account. This includes when you have accessed your account, and sites where you have used your OpenID and Information Cards.

Displaying 0 - 25 of 81 1 , 2 , 3 , 4 Next> Last>>

My Activities

Date ▲	Source ▼	Event ▼ ?	Result ▼	Action
2012-05-02	http://localhost:80/OpenId/examples/...	OpenID - Data Exchange	Authorized	Delete
2012-05-02	http://localhost:80/OpenId/examples/...	OpenID - Data Exchange	Authorized	Delete

Figure-5: Data exchange between RP and IdP in proposed model

VI. Comparison with Existing Models

Table 1 shows a concrete comparison between existing models and the proposed model in this paper.

Table1: comparison of proposed model with existing model

Method	Login any PC	Security	Expensive
MyOpenID’s_Personal_icon	Own	Safe	Inexpensive
VeriSign_and_IE7’s_Extended_Validation_Certificate_	Any	Safe	Expensive
Verisign and Firefox Seat Belt	Own	safe	Expensive
Vidoop’s_new_password_solution_	any	not very safe	Inexpensive
Jabber’s_authentication	Any	not very safe	Inexpensive
Proposed model in this paper	Any	Safe	free

VII. CONCLUSION

With exponential ground in web based applications, users have to create a number of usernames/passwords for interacting with these services. SSO, especially OpenID, is a good solution to this problem, but with its advantages it is vulnerable from phishing attacks. In this research we have described the phishing scenario in OpenID environment and presents new double factor based anti-phishing method for OpenID based SSO which is secure, free and very easy to implement in any OpenID enabled service. Authors believe this will give a hard time to intruders for phishing OpenID enabled websites integrated with this new protocol. A prototype system has been designed and the proposed protocol is tested against the possible phishing attacks, after a comprehensive testing and experimenting with different phishing methods, it is found that the proposed protocol is secure enough against the phishing attacks. We designed and evaluated a prototype system for validation of our model and found it a strong wall against phishing.

Competing Interests

The authors declare that they have no competing interests.

Authors' contributions

Asif and N.K.T have proposed and designed the improved protocol. Asif carried out most of the implementation part of prototype system development. Shahzad and shahbaz gave some good improvement suggestions in designing the protocol and implementation. All the authors read and approved the final version of manuscript.

Asif, Muhammad got his PhD in Computer Science and Information management Program, School of Engineering and Technology, Asian Institute of Technology Bangkok Thailand. He received his Master degree in Computer Science from Quaid-I-Azam University Islamabad, Pakistan. He is currently working as an Assistant professor and chairman of Computer Science Department at National Textile University Faisalabad. He worked as a Software Engineer in a project of Air traffic control system for Pakistan Air Force for a period of two years. After wards He joined the Asian Institute of Technology for his masters and PhD studies on a scholarship of Govt. of Pakistan. He was selected for an exchange program with National Institute of Informatics Japan where He carried out his part of research. Currently he is working as an Assistant Professor in department of Computer Science, National Textile University Faisalabad.

Nitin, Tripathi is Associate professor and leader ICT, School of Engineering and Technology Thailand. He obtained his PhD from Indian institute of Technology, India. He obtained his M. Tech. in Remote Sensing from Indian Institute of Technology, Kanpur, India. He is working as an Associate Professor in School of Engineering and Technology, Asian Institute of Technology Bangkok, Thailand. Dr. Tripathi is Editor in chief of International Journal of Geo Informatics and an author of several Journal articles and conferences. Dr. Tripathi has published a number of books in his field.

Acknowledgement

First author is heartily thankful to Dr. N.K. Tripathi whose encouragement, guidance and support from the initial to the final level enabled him to develop an understanding of the subject. Asif is thankful to his scholarship donor Higher Education Commission of Pakistan who supported them financially for their postgraduate studies. Authors are thankful to anonymous reviewers for their valuable suggestions and comments.

REFERENCES

[1] OpenID specification. Available online at http://www.openid.net. Last accessed on January, 2012.

[2] MyOpenID, OpenID provider. Available online at https://www.myopenid.com/. Last accessdon April. 2012.

[3] OpenID Authentication 2.0, OpenID Foundation, 2007. http://openid.net/specs/openid-authentication-2_0.html.Last accessdon April. 2013.

[4] Sun,S-T. Hawkey, K. Beznosov, K (2012).Systematically breaking andfixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures*Computers and Security.*

[5] Rafeeq Ur Rehman, The OpenID book, A comprehensive guide to OpenID protocol and running OpenID enabled web sites. 2008, Conformix Technologies IncOpenID. www.openid.net.

[6] OpenID and Phishing available online at “http://wiki.openid.net/w/page/12995230/Security” last accessed on April 24, 2012.

[7] HwanJin Lee, InKyungJeun, Kilsoo Chun and JunghwanSong(2008). A New Anti-Phishing Method in OpenID. *The Second International Conference on Emerging Security Information, Systems and Technologies.*

[8] Chun-Ying Huang a, _, Shang-PinMaa, Kuan-TaChen (2010). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications.*

[9] Levenshtein VI (1965). Binary codes capable of correcting spurious insertions and deletions of ones. *Problems of Information Transmission*; 1(1):8–17.

[10] Jae-Hwe You, Moon-Seog Jun (2010). A Mechanism to prevent RP Phishing In OpenID System. *9th IEEE/ACIS International Conference on Computer and Information Science*.

[11] QingxiangFeng, Kuo-Kun Tseng, Jeng-Shyang Pan, Peng Cheng, Charles Chen (2011). New Anti-phishing Method with Two Types of Passwords in Open ID System. *Fifth International Conference on Genetic and Evolutionary Computing.*

[12] Anti-Phishing Working Group. Phishing Activity Trends, November 2006. http://www.antiphishing.org/reports/apwg_report_november_2006.pdf.

[13] Dhamija R, Tygar JD, Hearst M (2006).Why phishing works. *In: CHI '06: proceedings of the SIGCHI conference on Human factors in computing systems*. New York, NY, USA: ACM; 2006. p. 581–90.

[14] Single Sign on (SSO), available online at , http://www.opengroup.org/security/sso/, last accessed on December, 2011.

[15] Jan De Clercq (2002). Single Sign-On Architectures, Infrastructure Security: *International Conference, InfraSec*.

[16] Daum OpenID. Available online at https://openid.daum.net/. Last accessed on April 23, 2012.

[17] Personal Identity Provider beta (VeriSign labs). Available online at https://pip.verisignlabs.com/. Last accessed on April 23, 2012.

[18] MyID.net.availalbe online at http://blog.myid.net/41. last accessed on April 25,2012.

[19] Vidoop. availalbe online at http://www.vidoop.com/.last accessed on April 25,2012.

[20] Jabber. availalbe online at http://www.jabber.org. . last accessed on April 25,2012.

[21] Yadis protocol Specification. Available online at http://yadis.org/papers/yadis-v1.0.pdf. Last accessed on February 23rd. 2010.

[22] VeriSign Labs Personal Identity portal server. "https://pip.verisignlabs.com/".Last accessd on April. 2013.

[23] QingxiangFeng, Kuo-Kun Tseng, Jeng-Shyang Pan, Peng Cheng and Charles Chen (2011). New Anti-phishing Method with Two Types of Passwords in OpenID System. Fifth International Conference on Genetic and Evolutionary Computing.

[24] OpenID site Directory, last accessed on August 15, 2012 available online at https://www.myopenid.com/directory. Last accessd on January. 2013.

[25] Ali Ghorbani& Mohammad Bakhtazmay Bonab (2013). Globalization and the Role of E-Commerce in Its Expansion. J. Basic. Appl. Sci. Res., 3(1)78-82.