Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037071

Article

Assessing Secure OpenID-Based EAAA Protocol to Prevent MITM and Phishing Attacks in Web Apps

Muhammad Bilal[1],*, Sandile C. Shongwe[2], Abid Bashir[3] and Yazeed Y. Ghadi[4]

[1]College of Computer Science and Technology, Zhejiang University, Hangzhou, 310027, China
[2]Department of Mathematical Statistics and Actuarial Science, Faculty of Natural and Agricultural Sciences, University of the Free State, Bloemfontein, 9301, South Africa
[3]Department of Computer Science, National Textile University, Faisalabad, 38000, Pakistan
[4]Department of Computer Science/Software Engineering, Al Ain University, Abu Dhabi, UAE

*Corresponding Author: Muhammad Bilal. Email: mbilal@zju.edu.cn

Received: 22 October 2022; Accepted: 30 January 2023

Abstract: To secure web applications from Man-In-The-Middle (MITM) and phishing attacks is a challenging task nowadays. For this purpose, authentication protocol plays a vital role in web communication which securely transfers data from one party to another. This authentication works via OpenID, Kerberos, password authentication protocols, etc. However, there are still some limitations present in the reported security protocols. In this paper, the presented anticipated strategy secures both Web-based attacks by leveraging encoded emails and a novel password form pattern method. The proposed OpenID-based encrypted Email's Authentication, Authorization, and Accounting (EAAA) protocol ensure security by relying on the email authenticity and a Special Secret Encrypted Alphanumeric String (SSEAS). This string is deployed on both the relying party and the email server, which is unique and trustworthy. The first authentication, OpenID Uniform Resource Locator (URL) identity, is performed on the identity provider side. A second authentication is carried out by the hidden Email's server side and receives a third authentication link. This Email's third SSEAS authentication link manages on the relying party (RP). Compared to existing cryptographic single sign-on protocols, the EAAA protocol ensures that an OpenID URL's identity is secured from MITM and phishing attacks. This study manages two attacks such as MITM and phishing attacks and gives 339 ms response time which is higher than the already reported methods, such as Single Sign-On (SSO) and OpenID. The experimental sites were examined by 72 information technology (IT) specialists, who found that 88.89% of respondents successfully validated the user authorization provided to them via Email. The proposed EAAA protocol minimizes the higher-level risk of MITM and phishing attacks in an OpenID-based atmosphere.

Keywords: Secure; user authentication; SSO; OpenID; phishing attack; MITM attack

1 Introduction

A Web system consists of Web services and Web applications necessary for its operations, e.g., Web portals, messengers, and websites. The main criterion for the efficient performance of any Web system is perceived latency which is the amount of time required to open a Web page. The factor that mainly affects perceived latency is a Web communication protocol [1–3]. Efficient working of Web communication induces a positive impact on a user and alternatively gives significant benefits to its owners. Irrespective of which type of website, whether it is an e-commerce website, a blog, a portfolio website, a piece of information, or a government website, all need good communication services. These websites face challenges in establishing a positive relationship with the users and making communication easier. However, all websites are not the same, so they encounter different challenges. Although Web communication dramatically affects our daily life in maintaining a business and running industries, theatres, and education systems. Its users have faced different problems. The main issue during web designing is a weak communication service, mainly overlooked by various agencies and corporations and has a backseat to other aspects. Apart from this, another factor that significantly affects Web communication is hijacking. Hence, it is necessary to protect the privacy and authentication of the user for wireless networks. Among all these, the authentication process ensures that the attackers cannot hack the user's communication data. In addition, for privacy preservation and authentication, secure communication is another research challenge for wireless networks [4–14].

This authentication process works by observing some protocols between a remote client and a server. The essential protocols include OpenID, lightweight directory access protocol, password authentication protocol, challenge-handshake authentication protocol, extensible authentication protocol, Kerberos, and others. Maintaining the user's identity remains a challenging task in information technology from a security point of view. Via digital identities, authentication and authorization can manage. In today's world, extensive use of the Internet and users' interest in creating different accounts create several problems, such as the formation of duplicate user profiles to access multiple online web applications. However, to evade the issue of identical profiles, OpenID has provided a lot of services. It is a standard and decentralized protocol in which identity is provided to the user to enable a website once. Then multiple websites can open by signing in to an existing account. This protocol is a practical, lightweight, convenient, and straightforward approach that manages the identities and removes the duplication profiles of web users on heterogeneous web applications. First, in 2005 its concept is arisen to solve different problems, and nowadays, it supports various renowned organizations, e.g., Facebook, Yahoo, Google, Microsoft, etc. Among all the reported OpenID benefits, strong authorized user authentication, cost-saving, the collaboration between OpenID-based industrial websites, transparently interchanging of data, and details about the hijacking, are the significant benefits of this protocol [15–19].

OpenID protocol is not only covered Web applications but also used in different mobile apps. However, the present research work focused chiefly on Web-based OpenID applications. This is why the word Web-based application used in the whole draft as a Hypertext Transfer Protocol (HTTP)-based application. The OpenID-based environment comprises three components-

- Identity Provider (IdP)/OpenID Provider (OP)
- Relying Party (RP)
- User Agents (UA)/User [19–30].

To sum up, Web communication is currently the primary area of study that links several embedded devices for data sharing and transfer (Fig. 1). It plays a vital role in running our daily life, business, education, agriculture, transportation, and other organizations. It is frequently seen that a considerable collaboration has been done through web-based environments and this technology significantly controls our business activities.

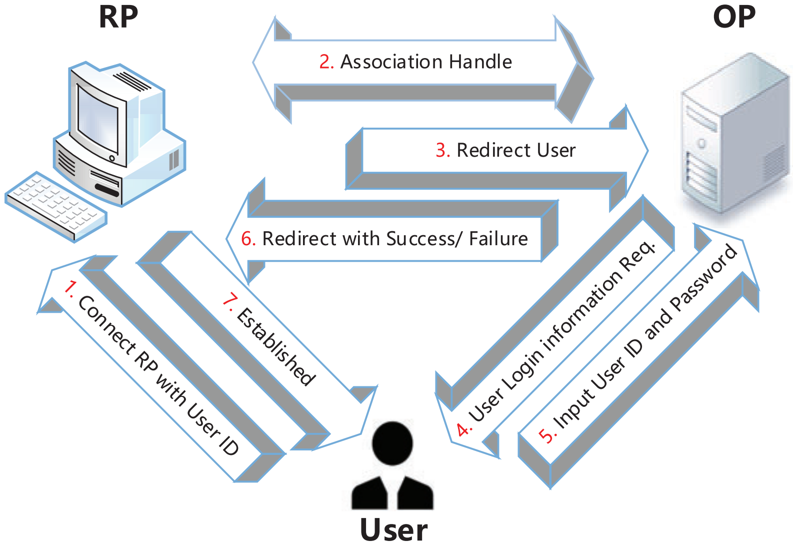

RP
OP
User
2. Association Handle
3. Redirect User
6. Redirect with Success/ Failure
1. Connect RP with User ID
7. Established
4. User Login information Req.
5. Input User ID and Password

Figure 1: OpenID-based atmosphere working process [18]

It is a challenging task to manage legitimate user identities in Web applications. Hackers are also working smartly due to the increased deployment of Web-based apps. A work environment based on OpenID may still attack by phishing and MITM Web attacks. Due to poor usability and security procedures, users are vulnerable to phishing and MITM attacks. Many researchers previously worked in this area, but it is a dominant issue. The OpenID-based advanced encrypted Email Authentication, Authorization, and Accounting (EAAA) protocol ensure security through the emails' authenticity and an additional Special Secret Encrypted Alphanumeric String (SSEAS). The present study aims to evaluate a safe triple-user authentication method in an OpenID-based working environment to address MITM and phishing attack issues.

The enhanced OpenID-based secure EAAA protocol is described in this article as a means of preventing MITM and phishing attacks. The legal user's identity is protected using the user secret fields' first Email's server-side encrypted link and SSEAS authentication on the RP side. Section 2 discusses the literature work on previously applied SSO security methods for avoiding MITM and phishing Web assaults. The designed secure triple OpenID-based EAAA protocol is detailed in Section 3. Section 4 denotes the implementation and discussion of a safe EAAA protocol in the experimental website and presents the testing results in the presence of hackers. Finally, in Section 5, future security recommendations are provided.

2 Literature Review/Related Work

Web-based attacks provide a significant challenge to both client and server-side Web applications. MITM and phishing attacks are frequent among Web users nowadays in an OpenID-based environment.

Some literature reports published by various researchers about these attacks and solutions to overcome these problems are presented in Table 1.

Table 1: Cybersecurity attacks and their solutions

Reports	References
Cybersecurity attacks	
In a MITM attack, an intruder intercepts messages and can change them until they are transformed into their destination.	[31–35]
Phishing is an activity in which the attacker uses social engineering-executing identity fraud methods. In this attack, a user's personal information can attain via a fake website and email address that an attacker sends to the user.	[36–42]
Solutions	
Single Sign-On (SSO)	
Many researchers are working to secure web-based applications using SSO authentication schemes. This authentication strategy uses a single login password to sign in to various websites.	[43–48]
Some published data regarding this protocol is as follows: Mittal et al. described a trustworthy model named DANE [DNS (Domain name sytems) Based authentication of named entities]-based Trust Plugin (DTP).	[49]
Bao et al. presented different schemes of trust enhancement of certificate services and then applied these schemes to the SSO system to get the credibility of SSO services.	[50]
Lin et al. presented a smartcard-based user-controlled SSO for privacy preservation in 5G-IoT (Internet of Things) telemedicine systems.	[51–53]
Authentication schemes to secure SSO-based atmosphere	
Single-factor authentication **MoScan** This method tests security vulnerabilities that are detected and reported for analysis. MoScan method performs all tasks state S0 to S5 and covers MITM attacks.	[54]
SSOScan This method automatically checks the top five vulnerabilities when the user integrates with the Facebook application.	[55]
MoSSOT This method tries to solve the main mobile user challenges such as manipulation of application state, heterogeneous applications, and unexpected behavior of applications.	[56,57]
Double-factor authentication Feng et al. described a new anti-phishing method with two types of passwords in open-ID systems. It is inexpensive but not very much secure in IdP-side web attacks.	[58]

(Continued)

Table 1: Continued

Reports	References
Wang et al. presented a One Time Password (OTP) that works only once to secure accounts from theft, and this scheme is widely used in banking sectors, internet gaming, and trading.	[59]
Similarly, the multi-level Open-ID user authentication system described by Wei et al. is based on two access request kinds, the authentication request and the operation request type.	[60]
Herley et al. have effectively created techniques to lower the risks of assaults through password-based solutions, such as ATM PINs.	[61]
Reese et al. suggested the Two-Factor Authentication (2FA) method that secured online banking websites. In their study, SMS, Time-Based One-Time Password (TOTP), progenerated codes, push, and Universal 2nd Factor (U2F) security keys are five standard 2FA techniques that researchers compare.	[62]
Shuwandy et al. described a unique authentication technique: a silent voice recording method that can effectively replace old voice recognition protocols. The main feature of the methodology is that it cannot be recorded by other devices except the user's phone and hence leaves no proof of password pattern.	[63]
Putri et al. described a token generation system based on the Ethereum blockchain platform with dApp to secure a two-factor authentication process.	[64]

3 Methodology

This research employs an applied research methodology. The enhanced OpenID-based user authentication model is designed with the support of three critical components of the OpenID working atmosphere: User-Agent (UA), Identity Provider (IdP), and Relying Party (RP). This model also includes an additional fourth component, an email server required for successful communication in an OpenID-based environment. The designed Email Authentication Authorization and Accounting (EAAA) OpenID-based user authentication protocol secures the OpenID URL user identity through the assistance of email authentication and Special Secret Encrypted Alphanumeric String (SSEAS). This work will discuss the SSEAS. In the SSEAS, the additional parameters field is restricted by six alphanumeric characters. The client must provide these alphanumeric characters in this form in any sequence. One alphanumeric character digit is chosen in any arrangement that is restricted.

- 0–9 (any number)
- A–Z (any Capital letter)
- a–z (any small letter)
- $+ - *$/% (any one operator)
- [ ] ( ) < > (Any one bracket)
- ! @ # $ ^ ? (Anyone special character)

According to the above sequence, the user chooses six digits from the above six restricted combinations in any form during registration time. For example, B6∗1@), 5+#Db>, (-B$7y, etc. But the valid user can use this sequence in any form. This step plays a vital role in user authentication.

Secondly, this study used an email server for appropriate user authentication in a well-organized and trustworthy OpenID-based atmosphere. The Email server provided an OpenID-based user authentication environment smartly and innovatively. The sequence of the proposed protocol is like this-

- OpenID Users Usage → Web-Based Application → OpenID-Based Environment → Web Communication Issues Faced → MITM and Phishing Attacks → Protection → Triple User Auth → Secure OpenID-Based Atmosphere Infrastructure.

According to the proposed model, triple-user authentication steps for protecting MITM and phishing attacks in the OpenID atmosphere are given below.

- Getting OpenID URL identity through Email
- Getting the SSEAS link with Identity Provider (IdP) response parameter via the valid user email address
- After authentication of the SSEAS parameter field authorized user received the Email of successful login in OpenID-Based environment
- The valid user also receives the Email when accessing the authorized user interface after completing the SSEAS authentication step.

The anticipated EAAA OpenID-based protocol is shown in Fig. 2, given below.

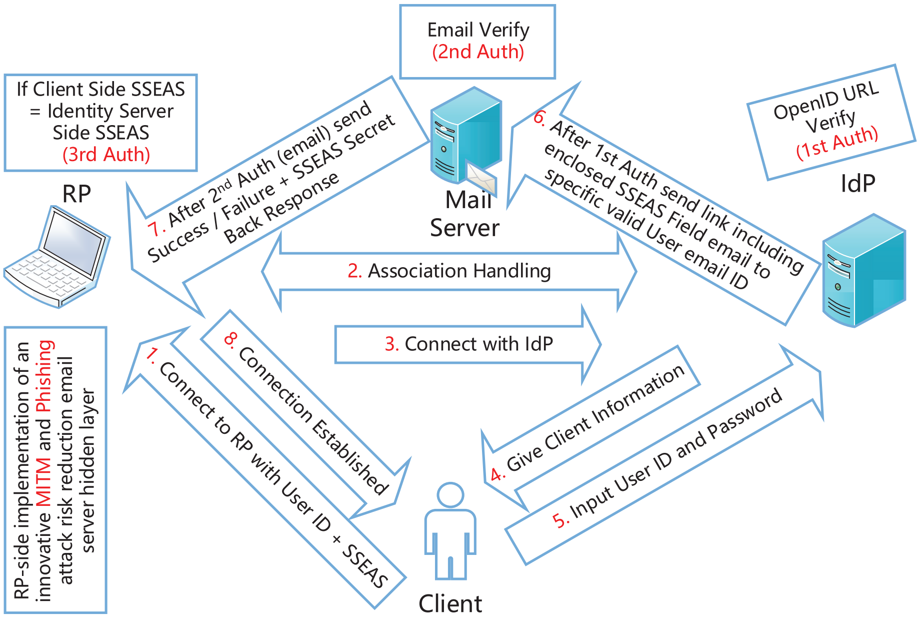

Email Verify
(2nd Auth)
If Client Side SSEAS = Identity Server Side SSEAS
(3rd Auth)
RP
7. After 2nd Auth (email) send Success / Failure + SSEAS Secret Back Response
Mail Server
6. After 1st Auth send link including enclosed SSEAS Field email to specific valid User email ID
OpenID URL Verify
(1st Auth)
IdP
2. Association Handling
3. Connect with IdP
RP-side implementation of an innovative MITM and Phishing attack risk reduction email server hidden layer
1. Connect to RP with User ID + SSEAS
8. Connection Established
4. Give Client Information
5. Input User ID and Password
Client

Figure 2: Proposed OpenID-based EAAA protocol

Different steps are involved for a productive EAAA OpenID-based user authentication environment mentioned below (Fig. 2).

- In the first step, the client connects with RP with a user ID and SSEAS parameter field.
- In the second step, RP associates with IdP to start communication with each other.
- In the third phase, an RP utilizes the Yadis discovery protocol and redirects the user requests to an IdP.
- In the fourth step, IdP requests the client (UA) to provide helpful information like ID.

- In the fifth step, the client provides the user details as an ID to the IdP side. In this step, the OpenID URL of a valid user check-in the IdP server database.
- After 1st authentication IdP server in the sixth step, a specific link is sent to them, including a remarkable SSEAS parameter field back response to the email server. If the user is valid, got the Email, and verified 2nd authentication.
- In the seventh step, after 2nd email verification, the authentication user clicks a specific link. In this client interface client-side SSEAS field match with the IdP side response from the email server-side match. If 3rd authentication is ok, a successful message is sent to the client; otherwise, rejected.
- In the eighth step, a successful connection is established between RP and the Client.

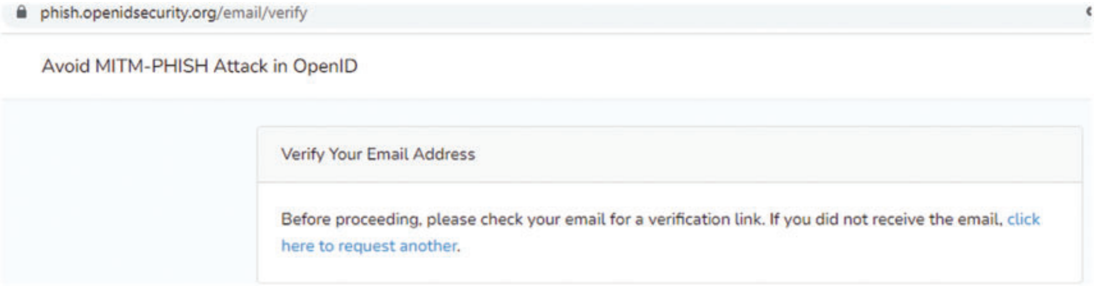
Triple authentication refers to first-user authentication using an OpenID URL carried out by the IdP. The second authentication is done on the email server side by getting a specific link with an additional back response of SSEAS from the IdP side. The third authentication is done on the RP side by comparing the client-side SSEAS parameter field with the SSEAS response from the IdP side to the email server side, and then the RP side matches. When the input fields for the request and response match, a successful connection is formed between the client side and the RP.

4 Implementation and Discussion

The robust Hypertext Preprocessor (PHP) Laravel framework used to build the proposed EAAA OpenID-based user authentication protocol. In this design protocol, two HTTPS secure domains were utilized from the EAAA protocol implementation point of view. The OpenID-enabled website does not facilitate users for any experiment due to security concerns. To resolve such security issues, an OpenID-based website is created in the present work from a user authentication point of view to avoid phishing and MITM attacks. This experiment used three main things like IdP/OP, OpenID User/Client/UA (User and RP act identically), and Email server. In this implementation cryptographic hash algorithm, SHA-256 is used innovatively and reliably.

4.1 OpenID Provider-Side

In this experiment, first of all, the user registers to get a unique OpenID URL by providing the most common Signup form information. In this Signup form, essential fields are essential from a new user registration point of view. The main field consists of Username, Country, Age, Password, Email address, and SSEAS details. When the user successfully fills out the Signup form, the valid user receives an email to get a unique OpenID URL identity. The verification of the correct user interface is shown in Fig. 3.



phish.openidsecurity.org/email/verify

Avoid MITM-PHISH Attack in OpenID

Verify Your Email Address

Before proceeding, please check your email for a verification link. If you did not receive the email, click here to request another.

Figure 3: Registration verification for valid user via email

When a legitimate user clicks on the link inside this registered confirmation email, it validates both the email address and the user's identity who used an OpenID URL. The illustration given below depicts Algorithm 1 for generating a distinct identity.

Server-Side Algorithm 1:

```
procedure UserRegistration()
if the Signup Form is successfully submitted, then
            Send an email Link to the user to complete the registration process
    if you click on the link in the Email, then
                    redirect to dashboard
    end if
 else
            redirect to Registration-Form with the error message
 end if
end procedure
```

A valid user utilizes the client-side interface for authentication after receiving a particular OpenID URL. If any user forgets his identity, then the valid user login through the email address and password on OpenID Provider (OP) side to receive his identity. The user forgets the OpenID URL identity interface, as shown in Fig. 4.

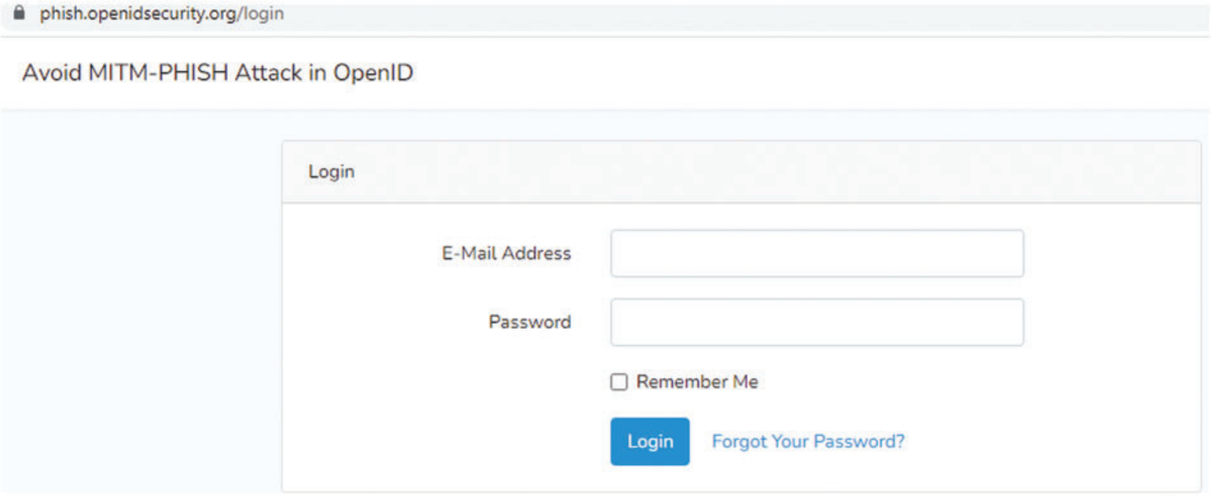


Figure 4: Getting OpenID URL identity in case of forgotten

Algorithm 2 illustrates an event when a valid user provides the correct email address and password and then sees the identity-relevant information.

Server-Side Algorithm 2:

```
procedure Login()
         if the Email and password are correct, then
                 login to dashboard
```

(Continued)

Server-Side Algorithm 2: Continued

```
        else
                redirect to *Login-Form* with the error message
  end if
end procedure
```

4.2 OpenID Client-Side

After getting the OpenID URL identity, the valid user interacts with OpenID client-side interface. In this implementation Client and RP sides behave the same thing. The first authentication of OpenID URL identity is done on the OP side and described in Algorithm 3.

Client-Side Algorithm 3: First and Second Authentication

```
procedure ManageSignIn()
        if the URL and PASSWORD are correct, then
                send an email Link to the user to complete the login process
          if you click on the link in the Email, then
            invoke 2nd Authentication Handler
          else
                  email link expires in 60 min
          end if
  else
          redirect to SignIn-Form with the error message
        end if
end procedure
```

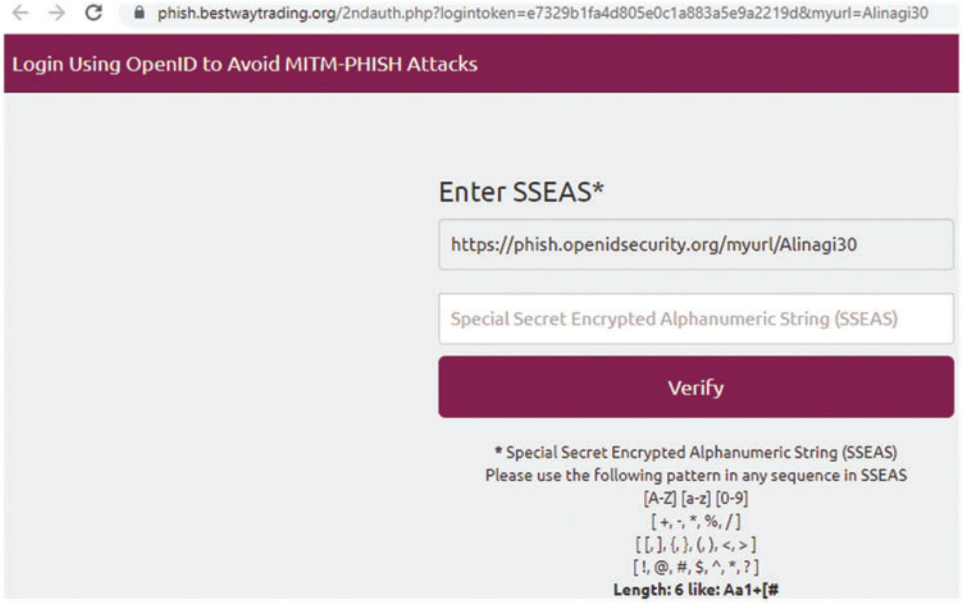
After 1st authentication user receives an email for 2nd user authentication, if the user is valid, then the OpenID provider sends a hidden email link for 2nd user authentication with the back response of the SSEAS parameter field. When a valid user clicks this link, move to another interface for SSEAS parameter authentication. In this authentication, set 60 min email link expiration option to better manage security.

The second authentication is done on the email server side in a hidden form. The third authentication interface is shown in Fig. 5, given below.

The 3rd SSEAS authentication-based algorithm is described below.

Client-Side Algorithm 4: Third Authentication

```
procedure 3rdAuthenticationHandler()
 if SSEAS is correct, then
                redirect to dashboard
 else
                redirect to SSEAS-Form with the error message
 end if
end procedure
```



phish.bestwaytrading.org/2ndauth.php?logintoken=e7329b1fa4d805e0c1a883a5e9a2219d&myurl=Alinagi30

Login Using OpenID to Avoid MITM-PHISH Attacks

Enter SSEAS*

https://phish.openidsecurity.org/myurl/Alinagi30

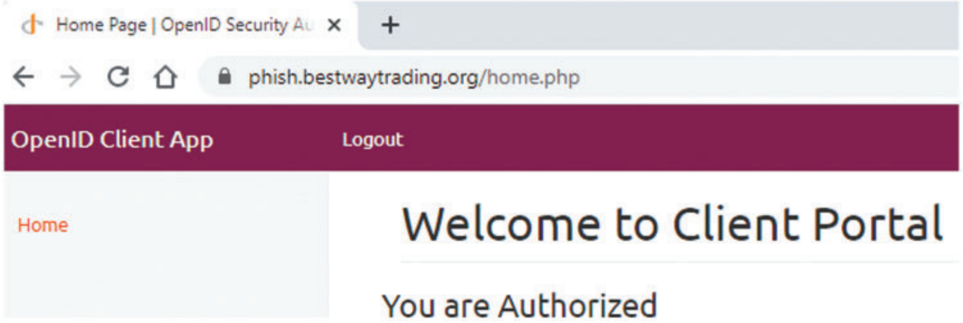
Special Secret Encrypted Alphanumeric String (SSEAS)

Verify

* Special Secret Encrypted Alphanumeric String (SSEAS)
Please use the following pattern in any sequence in SSEAS
[A-Z] [a-z] [0-9]
[+, -, *, %, /]
[[,], {, }, (,), <, >]
[!, @, #, $, ^, *, ?]
Length: 6 like: Aa1+[#

Figure 5: 3rd Authentication interface (SSEAS comparison)

Basically, in this step user OpenID Provider back response of the SSEAS field sends the client-side another interface of the 3rd authentication interface. Legal users access the authorized user interface if the client-side SSEAS parameter field matches the back reaction from the SSEAS parameter field; otherwise, a failure message is shown on the screen. If the user is valid, the authorized user accesses the main dashboard page, as shown in Fig. 6.



Home Page | OpenID Security Au

phish.bestwaytrading.org/home.php

OpenID Client App

Logout

Home

Welcome to Client Portal

You are Authorized

Figure 6: Authorized OpenID user interface

Finally, the legal users access the authorized OpenID-based environment after the secure authentication.

4.3 Cryptanalysis Study

Nowadays, most academics are working to secure the user identity in an OpenID-based environment. According to already available SSO-based techniques, security problems can solve with single, double, and multi-factor authentications. The users require security due to rapid progress in Web-based applications. Yet, the OpenID-based environment is still not secure against specific Web attacks such as MITM and phishing attacks.

A generalized cryptanalysis form of OpenID-based double factor user authentication threat situation against specific Web attacks is shown in Fig. 7.

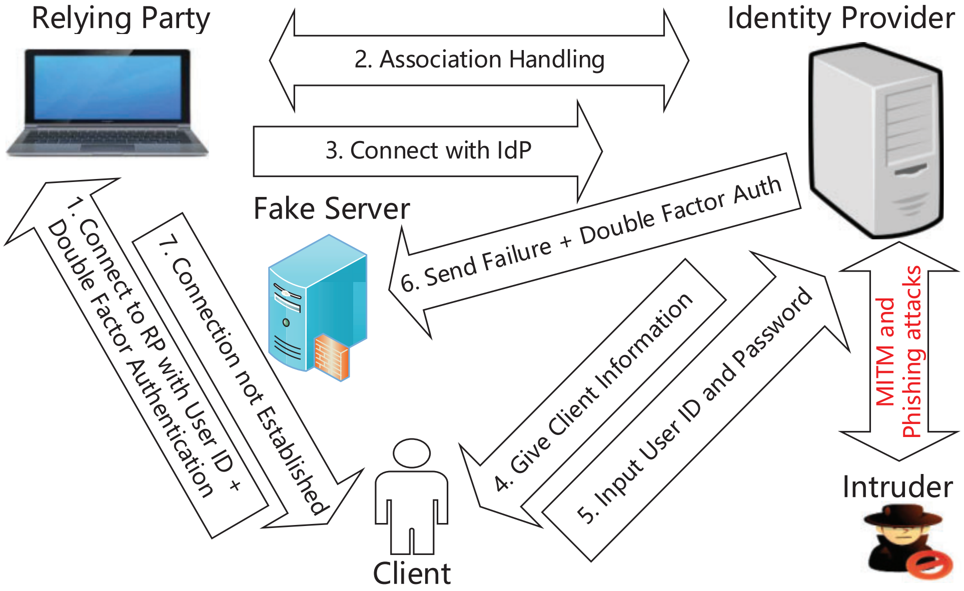

Relying Party
Identity Provider
2. Association Handling
3. Connect with IdP
Fake Server
6. Send Failure + Double Factor Auth
1. Connect to RP with User ID + Double Factor Authentication
7. Connection not Established
4. Give Client Information
5. Input User ID and Password
MITM and Phishing attacks
Intruder
Client

Figure 7: Generalized crypt form of 2-factor in MITM and phishing attacks in OpenID

Fig. 7 generalized cryptanalysis form of double authentication represents the MITM and phishing attacks in an OpenID-based environment. The mentioned specific Web-based attacks situation arises in step 6 when the user sends a double factor parameter for valid user authentication to a fake server. In this situation, an intruder can destroy valid user-sensitive data. Due to a weak security policy, intruders attack valid users and act as valid users. Therefore, fruitful communication cannot establish in an OpenID-based atmosphere. It is straightforward to break the implemented security solutions against MITM and phishing attacks in the presence of an intruder. Single, double, and multi-factor user authentication situations are already discussed in the literature review/related work. This study directs a critical review of single and double-factor user authentication in an OpenID-based atmosphere for sensing the Web attacks vulnerabilities in existing relevant research works. But all available solutions are still not secure against specific Web attacks like MITM and phishing attacks [28,30,65–67].

A security definition of this proposed cryptographic EAAA protocol proves that OpenID URL identity is safe against intruders. A secure cryptanalysis form of EAAA OpenID-based user authentication protocol design for avoiding MITM and phishing is shown below in Fig. 8.

Breaking the implemented security mechanism against MITM and phishing attacks is challenging. The present research has well-defined necessary computation secrecy of OpenID identity like valid user *Generate ID, Verify ID, Verify Email ID, and Verify SSEAS* parameters for authentications against theft. This study aims to prove that the proposed EAAA protocol meets this definition.

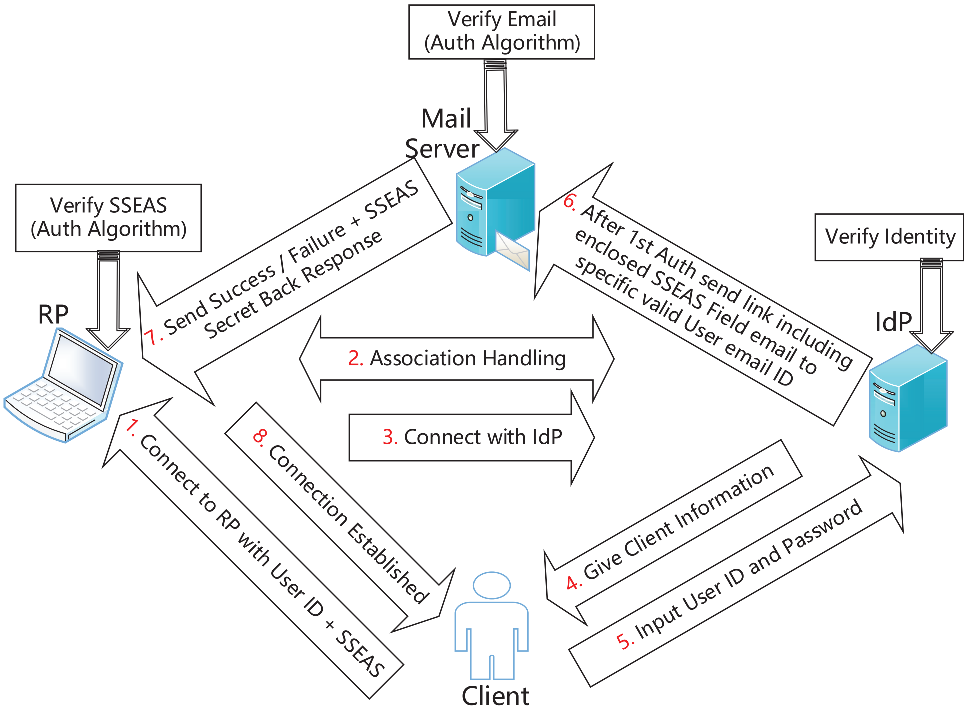

Verify Email
(Auth Algorithm)
Mail
Server
Verify SSEAS
(Auth Algorithm)
RP
Verify Identity
IdP
7. Send Success / Failure + SSEAS
Secret Back Response
6. After 1st Auth send link including
enclosed SSEAS Field email to
specific valid User email ID
2. Association Handling
3. Connect with IdP
1. Connect to RP with User ID + SSEAS
8. Connection Established
4. Give Client Information
5. Input User ID and Password
Client

Figure 8: Cryptanalysis of EAAA OpenID protocol against MITM and phishing attacks

- **Generate-ID**

Initially, the legal user gets a unique identity in this proposed secure EAAA OpenID-based atmosphere. The *Generate-ID* parameter is publicly accessible for all OpenID-based users to get a unique identity in the form of a URL. This identity is generated via email verification to avoid Web attacks from start to end.

- **Verify-ID**

Furthermore, the legal user identity is verified on Identity Provider (IdP) side. If the user identity is legal, then a second-factor authentication is still required to get complete access in EAAA OpenID-based atmosphere. After identity verification, the following process is to *Verify the SSEAS* field. After identity verification, a sensitive information link is sent to the email address with an SSEAS response to accomplish the authentication step. Email authentication is a hidden process for securing the OpenID-based environment against MITM and phishing attacks.

- **Verify-SSEAS**

Third, the legal user identity is verified on the RP side with another verification interface getting through Email. If the legal user's email side response of the SSEAS field confirms with the RP/user side SSEAS field, then the permitted user connects via a link and accesses a secure OpenID-based atmosphere; otherwise, a successful connection cannot establish. The SSEAS legal user authentication is done innovatively through safe algorithm implementation. The present scheme will be more secure and reliable because complete authentication is done on the RP side in the form of secure SSEAS form user authentication. This scheme is supplementary reliable and safe compared to already available solutions for avoiding phishing and session hijacking situations.

Assume that attacker has found the OpenID identity of *Generate ID* and *verified the ID* at Identity Provider (IdP) side. Then still present scheme will be secure because complete, valid user authentication is done on the Email server-side in the form of *Verify Email ID, and Verify SSEAS* authentication is done on the client side. OpenID-based EAAA user authentication protocol of the present research manages user authentication situations in a secure and trustworthy way. Hence, according to the contradictory study of cryptanalyses, this scheme will be more confident and reliable against phishing and MITM Web attacks.

The flow diagram of the EAAA OpenID-based user authentication protocol is shown in Fig. 9, given below. In this Diagram, S represents States (S0 to S8 Changes).

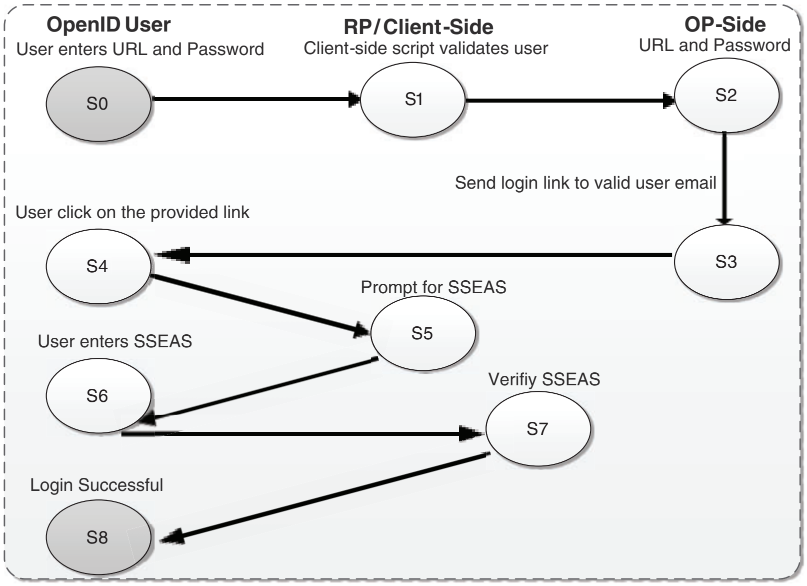


Figure 9: Flow diagram of EAAA OpenID-based user authentication protocol

Fig. 9. represents the flow of the EAAA OpenID-based protocol from initial to final state S0-S8.

According to the algorithmics mentioned above, OpenID-based EAAA user authentication protocol, a valid user's computational authentication time and additional security keys are calculated using Intel® Core™ i7-7500U 2.70 GHz, 8 GB RAM, 1 TB SAS-HDD. The crypto analysis for the valid user login authentication process is revealed in Table 2.

According to the algorithmic OpenID-based EAAA protocol, the first valid user URL and password authentication time have been calculated. The calculated time of all authentication steps is measured in milliseconds. The first identity time estimated is 204 ms. This is the first user authentication script time. Similarly, security keys of the first authentication of user identity have been calculated as only one. After the first user identity authentication, email link authentication in the email server and SSEAS field authentication time has been calculated together. The second hidden form authentication and SSEAS authentication time calculated is 135 ms. In the end, all valid user login authentication times are added. The total computational time for user login authentications is estimated at 339 ms. There are two security keys used in SSEAS authentication. In the second email authentication, one hidden automatic security key is used from a mail server. The previously available methods don't calculate computational time and security keys.

Table 2: Cryptoanalysis of EAAA protocol regarding user login authentication

Authentications	Operations	Computational time in milli seconds (ms)	Addition security keys (Token)
1	URL and password authentication (1st authentication)	204	1
2	Email link authentication (2nd authentication) When clicking on the email link, TOKEN and SSEAS is authenticated	135	2
	Total	**339 ms**	**3**

The proposed EAAA OpenID protocol user authentication responses time is faster than the previously used user authentication techniques, as shown in Table 3. This study manages two attacks such as MITM and phishing attacks. It gives 339 ms response time, which is higher than the already reported methods such as OAuth 2.0 and WSN methods.

Table 3: Summarize existing response times and the proposed method for auth request

References	Authentication types	Attack manage	Specifications	User authentication response time
1 [68]	Double	Man-In-The-Middle (MITM)	2-clickAuth (OAuth 2.0 method)	6250 ms
2 [44]	Triple	Brute force and Denial of service (DoS)	Enhanced user authentication protocol (WSN method)	450 ms
3 [17]	Triple	Phishing	Revers user authentication protocol	395 ms
4	**Triple**	**MITM and phishing**	**Proposed solution (EAAA OpenID method)**	**339 ms**

4.4 Experimental Website Testing Result

72 IT specialists have been hired to test experimental sites. The first stage was the training of the users that how they can use the designed triple authentication scheme and prevent from MITM and phishing attacks. After that analysis was carried out to check how many valid users successfully completed the login process. In this phase 1, if the intruders steal a valid user identity in the form of an OpenID URL, users can still not access the main authorized page because still authentication steps are left to authenticate the correct user completely. The second authentication is done on the email server side. The third authentication is done on the Client/RP side in a secure form. In the initial level of testing, better results were not obtained.

- OpenID URL (1st Authentication)
- Email Authentication (2nd Authentication)
- SSEAS (3rd Authentication)
- Authorized user Confirmation

The next stage was the analysis of successful login attempts in the mid of the session. In this middle-level phase, user's know how to use this system in a safe and reliable environment, therefor better results were received in this phase. And in the end, the final session user's successful login attempts were calculated and observed that valid users logged in quickly and securely on proposed experimental websites with tiny errors. In this level of testing, better results were received only due to the secure EAAA protocol authentication steps utilized. According to the final phase results, answers to all questions were received with satisfaction regarding valid user authentication against MITM and phishing and attack state.

The successful user login attempts are mentioned in Table 4.

Table 4: Testing of an experimental website regarding security aspects

User login success rate	1st authentication (OpenID-URL)	2nd authentication (Secure email received)	3rd authentication (SSEAS)	Valid user authorization (Via email)
Initial stage attempts	45	45	37	37
Middle stage attempts	53	53	46	46
Final stage attempts	59	59	56	56

The user's login successful attempt in the second authentication phase was approved by 93.65% of respondents and 88.89% of respondents recommended users' login successful attempts in the third authentication via Email received. All aspects of the authorized users' attempt ratio are shown in Fig. 10 below.

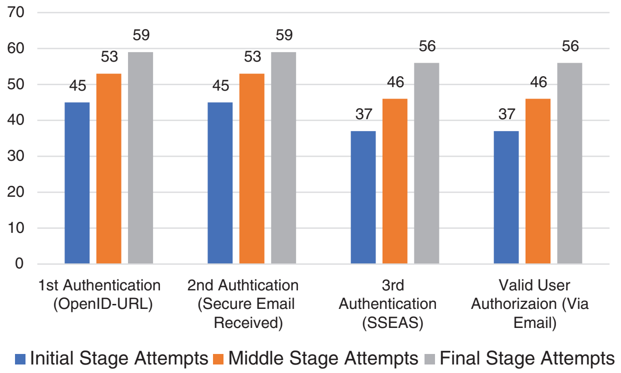


Figure 10: OpenID-based EAAA users login successful attempts

Table 5 provides an overview of the various SSO-based techniques. By comparing the proposed EAAA model to the current SSO techniques using all four security measures, Table 5 demonstrates that it is better.

Table 5: Evaluation of proposed EAAA OpenID protocol with available SSO methods

SSO based methods	Both client/RP and IdP side possible web-based attack chances	Email authentication	Authentication category	Trustworthy system
MoScan method [50]	The client-side is not secure in a MITM attack situation	×	*	L
SSOScan method [51]	Both IdP and RP-side are not secure in session, and MITM attacks	×	*	L
MoSSOT method [52]	Server-side not secure in MITM and session attacks	×	*	M
Anti-phishing two type password OpenID-based methods [54]	Both client and IdP-side are not very much safe in a phishing attack	×	**	M
OpenID-based one-time password (OTP) mechanism [55]	Both client and IdP-side are not very much secure in a reply and phishing attack situation	×	**	M
Anti-phishing OpenID-based method [28]	Both client and IdP-side are not very much secure in a phishing attack situation	×	**	M
BEAMAUTH anti-phishing bookmark solution [61]	Both client and IdP-side are not very much secure in a phishing attack situation	×	**	L
Anti-phishing QR-code SSO-based method [62]	Both client and IdP-side partially secure phishing and MITM attack situation	×	**	L
Anti-phishing scheme for cyberspace [30]	Both client and IdP-side are not very much secure in phishing & MITM attack situation	×	**	M

(Continued)

Table 5: Continued

SSO based methods	Both client/RP and IdP side possible web-based attack chances	Email authentication	Authentication category	Trustworthy system
OTP-SMS blockchain-based method [63]	Both server and RP-side are not very much secure in a MITM attack situation	×	∗∗	M
OpenID-based EAAA user authentication protocol (Proposed)	**Secure both sides from web-based attacks (MITM and phishing attacks)**	✓	∗∗∗	**H**

Notes: ∗Observations represent improved security features as compared to already available SSO protocol methods. [1]Email Authentication: No = ×; Yes = ✓. [2]Autentication Category: Single = ∗; Double = ∗∗; Triple = ∗∗∗. [3]Trustworthy System: Low = L; Medium= M; High = H.

In the end, it is summarized that the present work analyzed four main parameters:

- Web attacks such as phishing and MITM attacks are analyzed in the case of both client and IdP-sides.
- Email authentication aspect in all other existing systems is also analyzed in this study and it is concluded that reliable Email authentication and authorization processes only exist in this proposed method.
- Trustworthy-based system aspect is also analyzed in this study which is categorized into low, medium, and high levels.

It is concluded that this proposed method is very secure against phishing and MITM attacks compared to already implemented SSO methods.

5 Conclusion

Due to rapid development in Web-based applications, OpenID users faced several issues, such as phishing and MITM attacks. Considering this vital issue, researchers provide unique anti-phishing user authentication solutions. SSO is one of them, which works via single-factor, double-factor and multi-factor authentication protocols. However, some limitations are still present in the reported methodologies, such as response time, security issues, etc.

In the present research, the authorized user's OpenID URL identity is first protected by Email server-side authentication. Then a link is secretly provided by the email server for the additional parameter Special Secret Encrypted Alphanumeric String (SEEAS) authentication on the RP side. This proposed EAAA OpenID protocol user authentication responses time faster than the previously used user authentication techniques. Compared to existing cryptographic SSO protocols, the cryptographic EAAA protocol ensures that an OpenID URL's identity is secured from MITM and phishing attacks. As a result, Email server-side second authentication is safely performed using hidden layer logic. It is concluded that 72 IT specialists analyzed the testing sites and discovered that 88.89% of respondents correctly approved the user authorization via Email. Hence, the proposed Email Authentication, Authorization and Accounting (EAAA) protocol minimizes the MITM and phishing attacks in an

OpenID-based working atmosphere. Therefore, this work recommends that Internet identity layer problems of the OpenID atmosphere are resolved reliably.

The primary constraint of this research is that no well-known identity providers offered any researchers the ability to conduct experiments on already-running SSO-based websites. Future researchers also have room to address these enormous gaps. In the future, the Internet Identity layer will be more secure and reliable for cost-effectively improving the cryptographic algorithm's security step.

Funding Statement: This work is supported by the University of the Free State (UFS) Open Access Publication Fund.

Availability of Data and Materials: The data presented in this study are available upon request from the corresponding author. The data are not publicly available due to privacy concerns and the need to be made anonymous upon request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Pautasso, O. Zimmermann and F. Leymann, "Restful web services *vs.*"big "web services: Making the right architectural decision," in *Proc. 17th Int. Conf. on World Wide Web*, Beijing, China, pp. 805–814, 2008.

[2] L. Richardson and S. Ruby, "RESTful web services," O'Reilly Media, Inc., 2008. [Online]. Available: https://www.oreilly.com/library/view/restful-web-services/9780596529260/

[3] N. Naik, P. Jenkins, P. Davies and D. Newell, "Native web communication protocols and their effects on the performance of web services and systems," in *Proc. 2016 IEEE Int. Conf. on Computer and Information Technology (CIT)*, Nadi, Fiji, pp. 219–225, 2016.

[4] A. E. Atman Igrair and R. Yadav, "Authentication method for secure communication in mobile IP," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, pp. 340–345, 2017.

[5] R. -D. Silvia and B. Iryna, "The influence of online communication and web-based collaboration environments on group collaboration and performance," *Procedia Social and Behavioral Sciences*, vol. 46, pp. 935–943, 2012.

[6] A. Turrini, I. Soscia and A. Maulini, "Web communication can help theaters attract and keep younger audiences," *International Journal of Cultural Policy*, vol. 18, no. 4, pp. 474–485, 2012.

[7] E. M. Avram, "The importance of online communication in higher education," *Network Intelligence Studies*, vol. 3, no. 5, pp. 15–21, 2015.

[8] R. Lindemann, "The evolution of authentication," In: H. Reimer, N. Pohlmann and W. Schneider (Eds.), *ISSE 2013 Securing Electronic Business Processes*, pp. 11–19, Vieweg, Wiesbaden: Springer, 2013. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-658-03371-2_2

[9] A. Hiltgen, T. Kramp and T. Weigold, "Secure internet banking authentication," *IEEE Security & Privacy*, vol. 4, no. 2, pp. 21–29, 2006.

[10] T. Bhivgade, M. Bhusari, A. Kuthe, B. Jiddewar and P. Dubey, "Multi-factor authentication in banking sector," *International Journal of Computer Science and Information Technologies*, vol. 5, pp. 1185–1189, 2014.

[11] M. Turkanović, B. Brumen and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[12] L. Chen, F. Wei and C. Ma, “A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 4, pp. 704502, 2015.

[13] A. K. Das and A. Goswami, “A robust anonymous biometric-based remote user authentication scheme using smart cards,” *Journal of King Saud University-Computer and Information Sciences*, vol. 27, no. 2, pp. 193–210, 2015.

[14] R. Amin, S. H. Islam, G. Biswas and M. S. Obaidat, “A robust mutual authentication protocol for WSN with multiple base-stations,” *Ad Hoc Networks*, vol. 75, pp. 1–18, 2018.

[15] P. C. van Oorschot, “Authentication protocols and key establishment,” in *Computer Security and the Internet*, Cham: Springer, pp. 91–124, 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-33649-3_4

[16] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang and L. Shu, “Authentication protocols for internet of things: A comprehensive survey,” *Security and Communication Networks*, vol. 2017, pp. 6562953, 2017. https://doi.org/10.1155/2017/6562953

[17] M. Bilal, C. Wang, Z. Yu and A. Bashir, “Evaluation of secure openID-based RAAA user authentication protocol for preventing specific web attacks in web apps,” in *Proc. 2020 IEEE 11th Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, China, pp. 82–90, 2020.

[18] M. Bilal, M. Asif and A. Bashir, “Assessment of secure openID-based DAAA protocol for avoiding session hijacking in web applications,” *Security and Communication Networks*, vol. 2018, pp. 1–10, 2018.

[19] A. Muhammad and N. Tripathi, “Evaluation of openID-based double-factor authentication for preventing session hijacking in web applications,” *Journal of Computers*, vol. 7, no. 11, pp. 2623–2628, 2012.

[20] H. -K. Oh and S. -H. Jin, “The security limitations of SSO in openID,” in *Proc. 2008 10th Int. Conf. on Advanced Communication Technology*, Gangwon, Korea (South), pp. 1608–1611, 2008.

[21] G. D. Tormo, F. G. Mármol and G. M. Pérez, “Towards the integration of reputation management in openID,” *Computer Standards & Interfaces*, vol. 36, no. 3, pp. 438–453, 2014.

[22] A. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino *et al.,* “An authentication flaw in browser-based single sign-on protocols: Impact and remediations,” *Computers & Security*, vol. 33, pp. 41–58, 2013.

[23] P. Sovis, F. Kohlar and J. Schwenk, “Security analysis of openID,” in *Proc. Sicherheit*, Schutz und Zuverlässigkeit, Berlin, pp. 329–340, 2010.

[24] D. Fett, R. Küsters and G. Schmitz, “The web SSO standard openID connect: In-depth formal security analysis and security guidelines,” in *Proc. 2017 IEEE 30th Computer Security Foundations Symp. (CSF)*, Santa Barbara, CA, USA, pp. 189–202, 2017.

[25] A. Sharma, S. Sharma and M. Dave, “Identity and access management-A comprehensive study,” in *Proc. Int. Conf. on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, India, pp. 1481–1485, 2015.

[26] R. Rehman, “Get ready for OpenID,” OpenID Book, 2008. [Online]. Available: https://books.google.com.pk/books?id=i7yL2yCy-SUC&printsec=copyright&redir_esc=y#v=onepage&q&f=false

[27] J. Fishburn, “OpenID connect FAQ and Q&As,” 2019. [Online]. Available: (accessed on)

[28] M. Asif, M. S. Sarfraz, M. S. Ahmed and N. Tripathi, “A two factor based anti-phishing method in open ID,” *Journal of Basic and Applied Scientific Research*, vol. 3, no. 12, pp. 26–33, 2013.

[29] D. Kreutz, E. Feitosa, H. Cunha, H. Niedermayer and H. Kinkelin, “Increasing the resilience and trustworthiness of openID identity providers for future networks and services,” in *Proc. 2014 Ninth Int. Conf. on Availability, Reliability and Security*, Fribourg, Switzerland, pp. 317–324, 2014.

[30] H. Abbas, M. Qaemi Mahmoodzadeh, F. Aslam Khan and M. Pasha, “Identifying an openID anti-phishing scheme for cyberspace,” *Security and Communication Networks*, vol. 9, no. 6, pp. 481–491, 2016.

[31] S. Anand and V. Perumal, “EECDH to prevent MITM attack in cloud computing,” *Digital Communications and Networks*, vol. 5, no. 4, pp. 276–287, 2019.

[32] A. Mallik, “Man-in-the-middle-attack: Understanding in simple words,” *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, pp. 109–134, 2018.

[33] E. Ghazizadeh, Z. Shams Dolatabadi, R. Khaleghparast, M. Zamani, A. A. Manaf *et al.,* "Secure openID authentication model by using trusted computing," *Abstract and Applied Analysis*, vol. 2014, pp. 1–15, 2014.

[34] V. K. Yadav, R. K. Yadav, B. K. Chaurasia, S. Verma and S. Venkatesan, "MITM attack on modification of diffie-hellman key exchange algorithm," in *Proc. Int. Conf. on Communication, Networks and Computing*, Singapore, pp. 144–155, 2020.

[35] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN Journal of Engineering and Applied Sciences*, vol. 12, no. 22, pp. 6483–6487, 2017.

[36] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Computer & Security*, vol. 68, pp. 160–196, 2017.

[37] I. Vayansky and S. Kumar, "Phishing - challenges and solutions," *Computer Fraud & Security*, vol. 2018, no. 1, pp. 15–20, 2018.

[38] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, pp. 168, 2020.

[39] K. L. Chiew, K. S. C. Yong and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, 2018.

[40] B. B. Gupta, A. Tewari, A. K. Jain and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 1, pp. 3629–3654, 2017.

[41] A. A. Ubing, S. K. B. Jasmi, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "Phishing website detection: An improved accuracy through feature selection and ensemble learning," *International Journal of Advanced Computer Science and Applications*, vol. 10, pp. 252–257, 2019.

[42] K. Shaukat, A. Rubab, I. Shehzadi and R. Iqbal, "A socio-technological analysis of cybercrime and cyber security in Pakistan," *Transylvanian Review of Systematical and Ecological Research*, vol. 1, no. 3, pp. 4187–4190, 2017.

[43] T. Bazaz and A. Khalique, "Review on single sign on enabling technologies and protocols," *International Journal of Computer Applications*, vol. 151, no. 11, pp. 18–25, 2016.

[44] P. Prabu and T. Senthilnathan, "Secured and flexible user authentication protocol for wireless sensor network," *International Journal of Intelligent Unmanned Systems*, vol. 8, no. 4, pp. 253–265, 2020.

[45] O. Mir, M. Roland and R. Mayrhofer, "Decentralized, privacy-preserving, single sign-on," *Networks*, vol. 2022, pp. 1–18, 2022.

[46] A. -j. Cui, W. Wang, H. -f. Zhang, Y. -h. Ma, C. Li *et al.,* "Cross-domain single sign-on authentication of information security in network environment," *International Journal of Information and Communication Technology*, vol. 18, pp. 89–104, 2020.

[47] F. Magnanini, L. Ferretti and M. Colajanni, "Flexible and survivable single sign-on," in *Int. Symp. on Cyberspace Safety and Security*, Xi'an, China, pp. 182–197, 2022.

[48] C. Mainka, V. Mladenov, J. Schwenk and T. Wich, "Sok: Single sign-on security–an evaluation of OpenID connect," in *2017 IEEE European Symp. on Security and Privacy*, Paris, France, vol. 1, no. 1, pp. 251–266, 2017.

[49] N. Mittal, M. Misbahuddin and A. S. Mustafa, "Enabling trust in single sign-on using DNS based authentication of named entities," *International Journal of Microwave and Wireless Technologies*, vol. 1, no. 1, pp. 41–53, 2022.

[50] X. Bao, X. Zhang, J. Lin, D. Chu, Q. Wang *et al.,* "Towards the trust-enhancements of single sign-on services," in *Proc. 2019 IEEE Conf. on Dependable and Secure Computing (DSC)*, Hangzhou, China, pp. 1–8, 2019.

[51] T. -W. Lin, C. -L. Hsu, T. -V. Le, C. -F. Lu and B. -Y. Huang, "A smartcard-based user-controlled single sign-on for privacy preservation in 5G-IoT telemedicine systems," *Sensors*, vol. 21, no. 8, pp. 2880, 2021.

[52] M. Almulhim, N. Islam and N. Zaman, "A lightweight and secure authentication scheme for IoT based e-health applications," *International Journal of Computer Science and Network Security*, vol. 19, pp. 107–120, 2019.

[53] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas *et al.,* "A review on security challenges in internet of things (IoT)," in *Proc. 2021 26th Int. Conf. on Automation and Computing*, Portsmouth, Portsmouth, United Kingdom, pp. 1–6, 2021.

[54] H. Wei, B. Hassanshahi, G. Bai, P. Krishnan and K. Vorobyov, "MoScan: A model-based vulnerability scanner for web single sign-on services," in *Proc. 30th ACM SIGSOFT Int. Symp. on Software Testing and Analysis*, Virtual, Denmark, pp. 678–681, 2021.

[55] Y. Zhou and D. Evans, "SSOScan: Automated testing of web applications for single sign-on vulnerabilities," in *Proc. 23rd USENIX Security Symp.*, San Diego, CA, pp. 495–510, 2014.

[56] S. Shi, X. Wang and W. C. Lau, "MoSSOT: An automated blackbox tester for single sign-on vulnerabilities in mobile applications," in *Proc. 2019 ACM Asia Conf. on Computer and Communications Security*, Auckland New Zealand, pp. 269–282, 2019.

[57] K. Chaturvedi, A. Matheus, S. H. Nguyen and T. H. Kolbe, "Securing spatial data infrastructures for distributed smart city applications and services," *Future Generation Computer Systems*, vol. 101, pp. 723–736, 2019.

[58] Q. Feng, K. -K. Tseng, J. -S. Pan, P. Cheng and C. Chen, "New anti-phishing method with two types of passwords in openID system," in *Proc. 2011 Fifth Int. Conf. on Genetic and Evolutionary Computing*, Kitakyushu, Japan, pp. 69–72, 2011.

[59] H. Wang, C. Fan, S. Yang, J. Zou and X. Zhang, "A new secure openID authentication mechanism using one-time password (OTP)," in *Proc. 2011 7th Int. Conf. on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, pp. 1–4, 2011.

[60] J. Wei, M. Zhang, X. Ding and Y. Wang, "Research on multi-level security framework for openID," in *Proc. 2010 Third Int. Symp. on Electronic Commerce and Security*, Nanchang, China, pp. 393–397, 2010.

[61] C. Herley and P. van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 28–36, 2012.

[62] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron *et al.,* "A usability study of five two-factor authentication methods," in *Proc. Fifteenth Symp. on Usable Privacy and Security*, Santa Clara, CA, USA, pp. 357–370, 2019.

[63] M. L. Shuwandy, B. B. Zaidan and A. A. Zaidan, "Novel authentication of blowing voiceless password for android smartphones using a microphone sensor," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 44207–44243, 2022.

[64] M. C. I. Putri, P. Sukarno and A. A. Wardana, "Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application," *Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 74–85, 2022.

[65] B. Adida, "Beamauth: Two-factor web authentication with A bookmark," in *Proc. 14th Conf. on Computer and Communications Security*, Alexandria Virginia, USA, pp. 48–57, 2007.

[66] S. Mukhopadhyay and D. Argles, "An anti-phishing mechanism for single sign-on based on QR-code," in *Proc. Int. Conf. on Information Society (i-Society 2011)*, London, UK, pp. 505–508, 2011.

[67] E. Alharbi, D. Alghazzawi and A. Intelligence, "Two factor authentication framework using Otp-sms based on blockchain," *Transactions on Machine Learning and Artificial Intelligence*, vol. 7, no. 3, pp. 17–27, 2019.

[68] A. Vapen, D. Byers and N. Shahmehri, "2-ClickAuth optical challenge-response authentication," in *Proc. 2010 Int. Conf. on Availability, Reliability and Security*, Krakow, Poland, pp. 79–86, 2010.