I.J. Information Engineering and Electronic Business, **2022, 5, 42-50**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2022.05.05

Web Applications Login Authentication Scheme Using Hybrid Cryptography with User Anonymity

Bello Alhaji Buhari
Department of Mathematics, Computer Science Unit, Usmanu Danfodiyo University, Sokoto – Nigeria
E-mail: buhari.bello@udusok.edu.ng

Afolayan Ayodele Obiniyi
Department of Computer Science, Ahmadu Bello University, Zaria – Nigeria
E-mail: aaobiniyi@gmail.com

Received: 27 June 2021; Accepted: 13 July 2022; Published: 08 October 2022

Abstract: It is a common requirement for modern web applications as many if not all services that need personalization and control of access move online. Due to increase in these services becoming online, login authentications become targets to attackers. Therefore, there is need for secure and efficient web application login authentication schemes to ensure users access control, security and privacy. Present schemes have limitations such as users spent a lot of time browsing to create image portfolios than to create passwords and PINs, subject to active impersonation attack, some will only suit well for financial transaction system due to the TIC involved, some may have hash collisions, some require addition BLE device to be install and available on the authentication systems and cannot be used for higher data rates and long distance unlike cellular and WiFi devices, some involves reuse of password at single or multiple service providers which may lead to a password reuse attack called domino effect and some work well in application that needs to share permission with other applications like social media applications inform of APIs and improvising of user anonymity. We propose an improved web application login authentication scheme using hybrid cryptography with user anonymity. The improved scheme used blowfish – the most efficient private key algorithm, Elgamal – very secure public key algorithm and SHA-2 hash function combined together to enable high performance and security. The methods are thoroughly discussed and its security evaluated to show that it provides password protection, user privacy, perfect forward secrecy, mutual authentication and security against impersonation attack.

IndexTerms: Cryptography, Private key, Public key, Hash function, Authentication, Web login, Web application

1. Introduction

Web application login authentication is the process of validating the identity of a user. Users present their credentials, such as username and password, as evidence of their identity. Now we can quickly and easily login through Facebook, Google and a whole array of other services [1] . A user becomes authenticated when the presented credentials are valid and adequate. Actually, authentication does not determine which entity should be granted access, rather only verifies users are what they claim to be. So, it is only after users are authenticated they will have right to access resources based on their defined privileges.

It is a common requirement for modern web applications as many if not all services that need personalization and control of access move online. Including Web-based social media webapps like Whatsapp for computers, their feature makes it easier for users to share data and can be synchronized with their smartphone or user's computer [2] Due to increase in these services becoming online, login authentications become targets to attackers. Therefore, there is need for secure and efficient web application login authentication schemes to ensure users access control, security and privacy.

The standard way of user authentication, such as username and password, are no longer powerful enough to guarantee access control, security and privacy. Therefore, various researches have been conducted as solutions to these web login authentications such as [3, 4, 5, 6, 7, 8, 9, 10, 11].

PKI's big advantage over user names and passwords is that it lets individuals identify themselves in a way that does not itself compromise their actual identities [12].

Some previous schemes are trivial and users spent a lot of time browsing to create image portfolios than to create passwords and PINs [3], subject to active impersonation attack [4], some solutions schemes will only suit well for financial transaction system due to the TIC involved [5], some may have hash collisions which are virtually inescapable when hashing a random subset of a large set of possible keys [6] even though there are many collision resolution strategies to handle such events, some require addition BLE device to be install and available on the authentication systems and cannot be used for higher data rates and long distance unlike cellular and WiFi devices [7], some involves reuse of password at single or multiple service providers which may lead to a password reuse attack called domino effect [8] and some work well in application that needs to share permission with other applications like social media applications inform of APIs [9] .

This identified limitation motivated us to propose a an enhanced web application login authentication using hybrid cryptography with user anonymity. Private key cryptography is employed to enable the web server to create it only secrete key to used in encrypting the user identification to ensure user privacy. Public key encryption is employed to enable secure key distribution and make it hard for an attacker to compute secrete information dues computational Diffie-Hellman problem. Hashing is an essential method used for secure communication in the presence of attacker [13]. The proposed scheme is evaluated using cryptanalysis and proof that it provides password protection, user privacy, perfect forward secrecy, mutual authentication and security against impersonation attack.

2. Previous Works

Dhamija and Perrig in [3] addressed the human drawback to memorized secure passwords in login authentication. This is a primary weakness of knowledge-based authentication schemes. Therefore inspect the requirements of recognition-based system and proposed D ́ej`a Vu based on it rather than recall approach. Though the scheme is more reliable and easier to use than tradition password or PIN recall-based schemes it disallows users from choosing weak passwords and makes it difficult to write password or share it with others. Graphical based scheme is more susceptible to shoulder surfing than conventional traditional alphanumeric text password scheme [14]. This scheme is trivial and users spent a lot of time browsing to create image portfolios than to create passwords and PINs [15] for login authentication.

Van Der Horst and Seamons in [4] proposed a simple authentication for the web (SAW) to improve the automated email-based password login authentication. It removes the setup and management cost of passwords at medium to lower security web sites, provides single sign-on without a specialized identity provider, prevent all passive attacks and raises alarm for active attacks, allow easy, secure sharing and collaboration without passwords, provide intuitive delegation and revocation of authority and aid client-side auditing. But this scheme is subject to active impersonation attack [16]. This is because by providing a sufferer’s email address to a site, an attacker obtains an AuthTokenuser. Consequently, by observing the sufferer's unencrypted email traffic, the attacker acquires the associated AuthTokenemail and authenticates as the sufferer.

Tiwari et al. in [5] proposed a new wireless payment secure web authentication protocol based on multifactor authentication system using mobile device. They used transaction identification codes (TIC) and SMS to impose additional security to the traditional password login authentication approach. It is easy to use and implement and does not require any change in the infrastructure. This scheme will only suit well for financial transaction system due to the TIC involved.

Wang et al. in [6] proposed web login password authentication scheme based on single-block hash function to solve the problem that exists in traditional password authentication or digital signature in web login authentication. It is secure against replay attack, eavesdropping, messages modification and other common attacks. MD5 or SHA1 hash algorithm is used which are too cumbersome for web authentication of users and cost of computation is too high. But, hash collisions are virtually inescapable when hashing a random subset of a large set of possible keys [17] even though there are many collision resolution strategies to handle such events.

Varshney et al. in [7] found out that two factor authentication schemes such as Google 2 Step verification, SAASPASS, QR code, graphical password and push notification based login authentication schemes can be compromised using real time (RT) / control relay (CR) man-in-the-middle (MITM) phishing attacks. The hardware token involved require extra cost even though they are safe. Therefore, they proposed a secure authentication scheme that uses Bluetooth low energy devices for identification of users (login authentication). The scheme is location/client system independent and therefore withstands Bluetooth address spoofing attacks. But require addition BLE device to be install and available on the authentication systems. It cannot be used for higher data rates and long distance unlike cellular and WiFi devices and it is open to interception and attack [18].

Zeidler and Asghar in [8] proposed a flexible authentication scheme that allows users to reuse passwords securely for login authentication as well as for encrypted cloud storage at a single or multiple service providers called AuthStore. It allows users to securely store random login details such as web login passwords in the cloud. This reuse of password at single or multiple service providers may lead to a password reuse attack called domino effect [19] .

Lewi et al. in [9] developed two token-based methods for authentication. These tokens are based on certificate and “crypto auth token” for flexible verification due its public-key nature and more restrictive due to it asymmetric nature respectively. “Crypto auth token” rely on pseudorandom function to generate distributed independent keys for different identities. These methods work well in application that needs to share permission with other applications. That is, provision of permission to third-party applications. These applications involved social media applications. They are mostly in form of APIs.

Mohammed & Mehdi in [10] designed an algorithm that has the capability to achieve registration for login authentication or to access web applications safely. The proposed idea is based on the impression of Zero-knowledge proof.

Their result showed the importance of the proposed method by which the keys were managed and distributed in a safe and effective way. Even though their scheme is secure the MD5 hash function use is currently severely compromised [20] . And it does not guarantee user's privacy.

Gupta & Kapoor in [11] proposed hybrid model to secure data in web application. The AES algorithm is replaced by Blowfish security algorithm, which is faster than AES [21] and ECC algorithm is replaced by RSA algorithm. ECC algorithm can provide the same level of security afforded by RSA with a large modulus and corresponding large key. To confirm the originality of data MD5 algorithm is implemented and to authenticate the client modified Kerberos protocol is applied.

3. Methodology

The proposed web application login authentication is based on Elgamal cryptography, Blowfish and SHA-2. This section will discussed these techniques and algorithms.

3.1 Elgamal Cryptography

Elgamal is an asymmetric key algorithm developed by Taher Elgamal in the year 1984. It is based on Diffie-Hellman key exchange algorithm [22] and works over finite fields [23]. The algorithm is as follows [24]:

a. Parametric and key shaping algorithms

1. Select prime numbers large enough p so that the logarithm problem in Z_p is hard to solve.
2. Select $g \in Z_p^*$ as the primitive element.
3. Select the secret key x as a random number such that: $1 < x < p$
4. Generate public key y according to the formula:

$$y = g^x \bmod x \tag{1}$$

b. Encryption algorithms

Suppose the sender is Badawi, the receiver is Faika. The sender Badawi has the secret key: x_B and the public key is: y_B. The receiver Faika has a secret key of: and the public key is: x_F . Then, to send message M to Faila, with: , Sender Badawi will perform the following steps:

1. Select the random number k satisfactory: $1 < k < p$. Calculate the R value by the formula:

$$R = g^k \bmod p \tag{2}$$

2. Use public key of Faika to calculate:

$$C = M \times (y_F)^k \bmod p \tag{3}$$

3. Send the code (C, R) to the receiver Faika.

c. Decryption algorithms

To retrieve the original message *(M)* from the ciphertext *(C, R)* received, the receiver Faika performs the following steps:

1. Calculate the Z value by the formula:

$$Z = R^{xF} \bmod p = g^{k,xF} \bmod p \tag{4}$$

2. Calculate the inverse of Z:

$$Z^{-1} = (g^{k,xF})^{-1} \bmod p = g^{-k,xF} \bmod p \tag{5}$$

3. Restore initial message (M):

$$C \times Z^{-1} \bmod p \tag{6}$$

3.2 Blowfish Cryptography

Blowfish is a symmetric cipher algorithm that can be effectively used for encryption and safeguarding of data [21]. It is a 64-bit block cipher and variable length key developed by Bruce Schneier [25]. The basic algorithm for Blowfish is as follows [21]:

```
Divide X into two 32-bit halves XL and XR
For i=1 to 16:
   XL = XL Pi
   XR = F (XL) XR
   Swap XL and XR
End for
Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)
```

3.3 SHA-2 Cryptography

The SHA-2 was finalized in 2009 by the National Institute of Standards and Technology (NIST). It is actually a set of cryptographic hash algorithms defined by the National Institute of Standard and Technology (NIST) in the Secure Hash Standard (SHS) for being employed by the U.S [26]. The two basic variants are SHA-256 and SHA-512, which are the same algorithm, applied to dissimilar word lengths. SHA-256 operates on 32-bit words, whereas SHA-512 works on 64-bit words.

The detail operation of SHA-2 hash block [27] is shown in Fig. 1. The operations of the compressor and expander mainly consist of arithmetic additions, bit-permutation operations, and bitwise rotations. In round iteration of SHA-2, the compression results are temporarily stored and updated in working variable registers. The input message of hash block, which is also referred as padded data block (PDB), is handled by expanders to generate the message word (Wt).

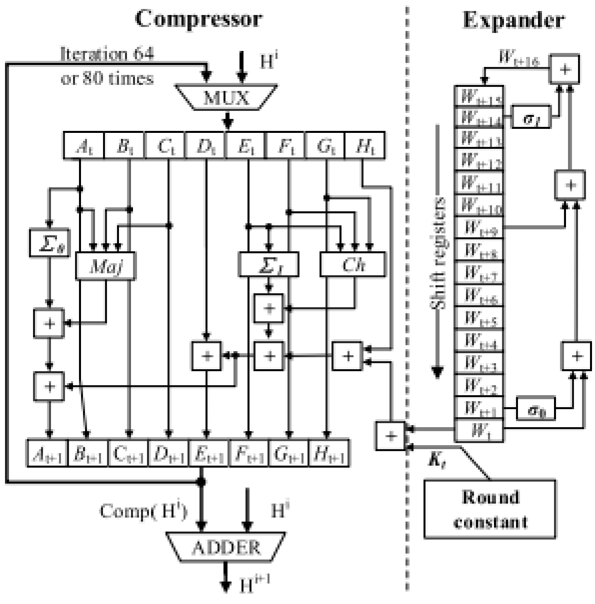

Fig.1. The description of SHA-2 hash block [26].

4. Proposed Web Applications Login Authentication Scheme

In this section, we proposed a new web application login authentication scheme using hybrid cryptography. Also, privacy will be ensured through anonymity. The private key algorithm used is blowfish due to its efficiency. The public key algorithm used is Elgamal dues it expandability and security and the SHA-2 will be used as the hash function algorithm. It consists of five (5) phases namely: initialization, registration, login, authentication and change password. These phase will discussed in details in the remaining sub-sections of this section.

4.1 *Initialization Phase*

The web server WS does the following before users can able register in order to have legitimate access to the web application:

1. Select two prime numbers p and q such that

$$p = 2q + 1 \tag{7}$$

2. Select a generator g of Z_q^*
3. Select a cryptographic hash function $h(\bullet)$ that is SHA-2
4. Select $x \in Z_q^*$ as its secrete key
5. Select a private key algorithm like Blowfish; $E_y(\bullet)$ for encryption and $D_y(\bullet)$ for decryption using key y
6. Decides the format of identity UN_i

This can be shown in Fig. 1.

User (U_i)	**Web Server (WS)**
	Initialization Phase *S chooses p and q where* $p = 2q + 1$ $x \in Z_q^*$

Fig. 1. Initialization Phase

4.2 *Registration Phase*

For a user U_i to register with the web application server he/she does the following:

1. U_i selects his/her identity UN_i and password PW_i in the specified format and submit to WS securely.
2. U_i selects a random number b_i
3. WS encrypt the identity UN_i as

$$EUN_i = E_x(UN_i) \tag{8}$$

4. WS computes security parameters

$$P_i = (EUN_i)^{h(x, PW_i)} \bmod p \tag{9}$$

5. WS stores $\{P_i, EUN_i, h(\bullet)\}$ to the database

This can be shown in Fig. 2.

User (U_i)		**Web Server (WS)**
Registration Phase *Choose* UN_i, PW_i & b_i	$\{UN_i, PW_i\}$ →	$P_i = (EUN_i)^{h(x, PW_i)} \bmod p$ $EUN_i = E_x(UN_i)$
Store $\{P_i, EUN_i, h(.)\}$ *the databse*	← $\{P_i, EUN_i, h(.)\}$	

Fig. 2. Registration Phase

4.3 *Login Phase*

If a user U_i wants to login to the web application server WS he/she performs the following:

1. Provides identity UN_i and password PW_i
2. U_i computes:

$$C_i = P_i \,|\, (EUN_i)^{PW_i \bmod p} \tag{10}$$

$$D_i = (EUN_i)^{b_i \bmod p} \tag{11}$$

$$W_i = C_i D_i \bmod p \tag{12}$$

$$M_i = h(EUN_i, C_i, D_i, W_i\ ) \tag{13}$$

3. U_i sends the login request message $\{EUN_i, C_i, D_i, W_i\}$ to WS

This can be shown in Fig. 3

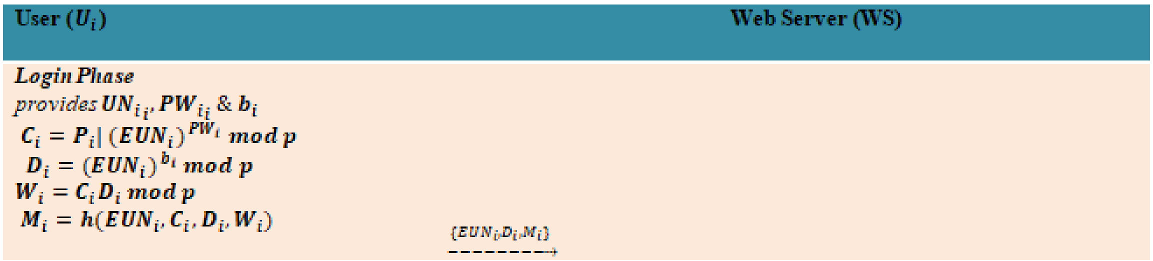

Fig. 3. Login Phase

4.4 *Authentication Phase*

WS and U_i perform the following steps to authenticate each other

1. On receiving the login request message WS checks the format of identity UN_i, if UN_i is valid it goes to the next step; otherwise it rejects the login request.
2. WS computes:

$$C_i = (EUN_i)^x \bmod p \tag{14}$$

$$W_i^{'} = C_i D_i \bmod p \tag{15}$$

$$M_i^{'} = h(EUN_i, C_i, W_i) \tag{16}$$

3. WS compares M_i' and M_i, if they are equal U_i is authenticated; otherwise the login request is rejected
4. WS computes:

$$M_s = h(EUN_i, W_i^{'}) \tag{17}$$

   And sends the mutual authentication message $\{EUN_i, M_s\}$ to U_i

5. On receiving the message, U_i check EUN_i and compares M_s and M_i, if they are equal WS is also authenticated; otherwise the login request is rejected.
6. Now, both U_i and WS compute the session key

$$sk = h(W_i) = h(W_i^{'}) \tag{18}$$

This can be shown in Fig. 4:

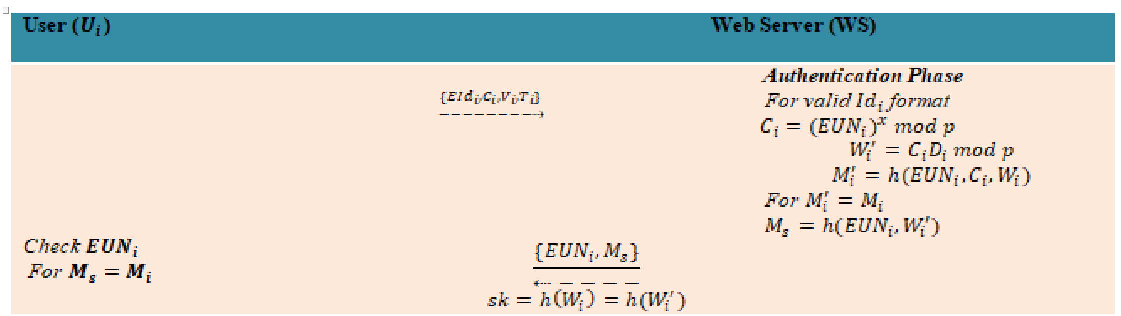

Fig. 4. Authentication Phase

4.5 *Change Password Phase*

User U_i performs the following steps to change his/her her existing password PW_i to a new password $(PW_i)_{new}$. We assume that the user is already being authenticated before he/she can be able to change password.

1. The user U_i provides his/her new password $(PW_i)_{new}$
2. WS re-computes security parameters

$$(P_i)_{new} = (EUN_i)^{h(x,(PW_i)_{new})} \tag{19}$$

3. WS replaces P_i with $(P_i)_{new}$ on the EUN_i data row in the database

This can be shown in Fig. 5

User (U_i)	Web Server (WS)
Change Password Phase U_i *selects* $(PW_i)_{new}$ $(P_i)_{new} = (EUN_i)^{h(x,(PW_i)_{new})}$	*replaces* P_i *with* $(P_i)_{new}$ *on the* EUN_i *data row in the database*

Fig. 5. Change Password Phase

4. Security of the Proposed Scheme

In this section, we analyse the security of the proposed scheme. The security of the proposed scheme is based on the combination of private key cryptography, public key cryptography and hash function. Also, user anonymity is imposed to ensure user privacy. The proposed scheme provides password protection, user privacy, perfect forward secrecy, mutual authentication and security against impersonation attack.

4.1 *Password Protection*

The proposed web application login authentication scheme provides password protection. This is accomplished by hashing the password together with the web server secrete key as $h(x, PW_i)$ and the password is neither stored in the database nor in the web server. Also, P_i is computed as $P_i = (EUN_i)^{h(x,PW_i)} \bmod p$ based on discrete logarithm problem. So, it very hard to get $h(x, PW_i)$ from P_i. And $h(x, PW_i)$ is a one hash function so, PW_i cannot be known.

4.2 *User Privacy*

In our scheme, the user registration information, $\{P_i, EUN_i, h(\bullet)\}$, stored on the database, the login request message $\{EUN_i, D_i, M_i\}$ send to WS and mutual authentication message $\{EUN_i, M_s\}$ send to U_i do not contain open static identity of the use U_i. Therefore, an attacker cannot easily know which user is connecting with the web server from the database and these messages.

4.3 *Perfect Forward Secrecy*

Forward secrecy ensures that the session key generated remains unbroken even after the disclosure of systems secret key. In the proposed scheme, U_i and WS generate the session key $sk = h(W_i) = h(W_i^{'})$ and $W_i = C_i D_i \bmod p = W_i^{'}$. To obtain the session key, the attacker has to compute $C_i D_i$ from $C_i = (EUN_i)^x \bmod p$ and $D_i = (EUN_i)^{b_i} \bmod p$. He has to solve computational Diffie-Hellman problem. The attacker cannot obtain the session even if he/she knows the U_i and WS secrete key.

4.4 *Mutual Authentication*

A good password authentication scheme ensures mutual authentication, meaning that, not only can the server verify the legality of user, but the user can also verify the legality of server. In the proposed protocol, the server WS and the use U_i mutual authentication each other by sending message $\{EUN_i, D_i, M_i\}$ and $\{EUN_i, M_s\}$ respectively. No one other than the legal user can create a valid message $\{EUN_i, D_i, M_i\}$. On the other hand, only legal server can create a valid $\{EUN_i, D_i, M_i\}$.

5. Security against Impersonation Attack

To impersonate as U_i., the attacker must generate valid login message $\{EUN_i, D_i, M_i\}$, similarly, to impersonate as WS attacker must be able to generate valid mutual authentication message $\{EUN_i, M_s\}$. Similarly, to generate valid mutual message attacker needs WS secrete key x. so, the proposed scheme resist user and web server impersonation attack.

6. Conclusion

It is a common requirement for modern web applications as many if not all services that need personalization and control of access move online. Due to increase in these services becoming online, login authentications become targets to attackers. Therefore, there is need for secure and efficient web application login authentication schemes to ensure users access control, security and privacy.

Various researches has been conducted as solutions to these web login authentications. PKI's big advantage over user names and passwords is that it lets individuals identify themselves in a way that does not itself compromise their actual identities.Some previous schemes are trivial and users spent a lot of time browsing to create image portfolios than to create passwords and PINs, subject to active impersonation attack, some solutions schemes will only suit well for financial transaction system due to the TIC involved, some may have hash collisions which are virtually inescapable when hashing a random subset of a large set of possible keys even though there are many collision resolution strategies to handle such events, some require addition BLE device to be install and available on the authentication systems and cannot be used for higher data rates and long distance unlike cellular and WiFi devices, some involves reuse of password at single or multiple service providers which may lead to a password reuse attack called domino effect and some work well in application that needs to share permission with other applications like social media applications inform of APIs.

Therefore, we propose a new web application login authentication scheme using hybrid cryptography with user anonymity. The private key algorithm used is blowfish due to its efficiency. The public key algorithm used is Elgamal dues it expandability and security and the SHA-2 will be used as the hash function algorithm. Also, privacy will be ensured through anonymity. This proposed scheme is evaluated using cryptanalysis and proof that it provides password protection, user privacy, perfect forward secrecy, mutual authentication and security against impersonation attack.

References

[1] Patel, S., Sahoo, A., Mohanta, B. K., Panda, S. S., & Jena, D. (2019, March). DAuth: A Decentralized Web Authentication System using Ethereum based Blockchain. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-5). IEEE.

[2] Anwar, N., & Supriyanto, S. (2019). Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *8*(3), 206-212.

[3] Dhamija, R., & Perrig, A. (2000, August). Deja Vu-A User Study: Using Images for Authentication. In *USENIX Security Symposium* (Vol. 9, pp. 4-4).

[4] Van Der Horst, T. W., & Seamons, K. E. (2007, September). Simple authentication for the web. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007* (pp. 473-482). IEEE.

[5] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S. J., & Sanyal, S. (2011). A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *arXiv preprint arXiv:1111.3010*.

[6] Wang, S. Q., Wang, J. Y., & Li, Y. Z. (2013). The web security password authentication based the single-block hash function. *IERI Procedia*, *4*, 2-7.

[7] Varshney, G., Misra, M., & Atrey, P. (2017, October). A new secure authentication scheme for web login using BLE smart devices. In *2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)* (pp. 95-98). IEEE.

[8] Zeidler, C., & Asghar, M. R. (2018, August). AuthStore: Password-based Authentication and Encrypted Data Storage in Untrusted Environments. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 996-1001). IEEE.

[9] Lewi, K., Rain, C., Weis, S. A., Lee, Y., Xiong, H., & Yang, B. (2018). Scaling Backend Authentication at Facebook. *IACR Cryptology ePrint Archive*, *2018*, 413.

[10] Mohammed, S. J., & Mehdi, S. A. (2020). Web application authentication using ZKP and novel 6D chaotic system. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(3), 1522-1529.

[11] Gupta, N., & Kapoor, V. (2020). Hybrid cryptographic technique to secure data in web application. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(1), 125-135.

[12] Garfinkel, S. L. (2003). Email-based identification and authentication: An alternative to PKI?. *IEEE security & privacy*, *1*(6), 20-26.

[13] Thomas, C. G., & Jose, R. T. (2015). A comparative study on different hashing algorithms. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(7), 170-175.
[14] Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*.
[15] Suresh, S., & Prakash, G. (2015). On reviewing the limitations of graphical password scheme. *Journal of Computer Science and Engineering Research: 2014*, *1*(1), 31-35.
[16] Harding, A., Van Der Horst, T. W., & Seamons, K. E. (2008, March). Wireless authentication using remote passwords. In *Proceedings of the first ACM conference on Wireless network security* (pp. 24-29).
[17] Nimbe, P., Frimpong, S. O., & Opoku, M. (2014). An Efficient Strategy for Collision Resolution in Hash Tables. *International Journal of Computer Applications*, *99*(10), 35-41.
[18] Rfwireless-world.com. (2020). *Advantages of BLE (Bluetooth Low Energy) | disadvantages of BLE (Bluetooth Low Energy)*. [online] Available at: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-BLE-Bluetooth-Low-Energy.html [Accessed 5 Feb. 2020].
[19] Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75-78.6
[20] Jacob, N. M. (2016). Vulnerability of data security using MD5 function in php database design. *International Journal of Science and Engineering (IJSE)*, *1*(1), 11-15.
[21] Buhari, B. A., Obiniyi, A. A., Sunday, K., & Shehu, S. (2019). Performance evaluation of symmetric data encryption algorithms: Aes and blowfish. *Saudi Journal of Engineering and Technology*, *4*, 407-414.
[22] Al Hasib, A., & Haque, A. A. M. M. (2008). A comparative study of the performance and security issues of AES and RSA cryptography. In*Convergence and Hybrid Information Technology. ICCIT'08. Third International Conference on* (Vol. 2, pp. 505-510). IEEE.
[23] Singh, R., & Kumar, S. (2012). Elgamal's algorithm in cryptography.*International Journal of Scientific & Engineering Research*, *3*(12), 1-4.
[24] Toan, N. D. & Hong B. T. (2017) Building Background to the Elgamal Algorithm *International Journal of Mathematical Sciences and Computing(IJMSC)*, Vol.3, No.3, pp.39-49. DOI: 10.5815/ijmsc.2017.03.04.
[25] Rubab, S., & Javed, Y. (2015). Efficient Image Steganogrphic Algorithms Utilizing Transforms: Wavelet and Contourlet with Blowfish Encryption. *International Journal of Computer Network & Information Security*, *7*(2).
[26] Buhari, B. A., Mubarak, A., Bodinga, B. A., & Sifawa, M. D. (2022). Design of a Secure Virtual File Storage System on Cloud using Hybrid Cryptography. *International Journal of Advanced Networking and Applications*, *13*(5), 5143-5151.
[27] Zhang, Y., He, Z., Wan, M., Zhan, M., Zhang, M., Peng, K., ... & Gu, H. (2021). A new message expansion structure for full pipeline SHA-2. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *68*(4), 1553-1566.

Authors' Profiles

Bello Alhaji Buhari, Obtained B.Sc. in Computer Science at Usmanu Danfodiyo UniversitySokoto – Nigeria and M.Sc. in Computer Science at Ahmadu Bello University Zaria –Nigeria. He is now pursuing Ph.D. in Computer Science at Usmanu Danfodiyo UniversitySokoto – Nigeria. He is a Lecture in the Department of Computer Science, Usmanu Danfodiyo University Sokoto – Nigeria since 2004. His research interest include: Web Security and Cryptography.

Prof. A.A. Obiniyi received his Ph.D degree in Computer Science from Ahmadu Bello University (ABU), Zaria in Kaduna State of Nigeria in 2009. He is a Professor of Computer Science and a member of Nigeria Computer Society (NCS), Internet Society (ISOC), Academia in Information Technology Professionals (AITP), Institute of Electrical and Electronic Engineers (IEEE) and a Chartered member of Computer Professionals (Registration Council of Nigeria)[CPN]. He lectures in the Department of Computer Science of Ahmadu Bello University, Zaria – Kaduna State. Presently, he is co-supervising eight Ph. D. and thirteen Master of Computer Science students with many Ph.D. and Master of Computer Science scholars completed their studies. He also has many publications to his credit. His research interests include Computer Networking, Cyber Security and Database Development among others.

How to cite this paper: Bello Alhaji Buhari, Afolayan Ayodele Obiniyi, " Web Applications Login Authentication Scheme Using Hybrid Cryptography with User Anonymity", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.14, No.5, pp. 42-50, 2022. DOI:10.5815/ijieeb.2022.05.05