Web application authentication using ZKP and novel 6D chaotic system

Shatha J. Mohammed[1], Sadiq A. Mehdi[2]
[1]Department of CS, College of Science, Mustansiriyah University, Iraq
[2]Department of CS, College of Education, Mustansiriyah University, Iraq

Article Info

Article history:

Received May 1, 2020
Revised Jul 23, 2020
Accepted Aug 2, 2020

Keywords:

Authentication
Chaotic System
NIST
Password
Web application
ZKP

ABSTRACT

Text password has long been a dominant approach to user authentication used by a huge quantity of Internet services. Web applications are now widely used for the implementation of a range of significant services. The securing of such applications has thus become a significant process. Currently the frequent use of passwords and the need for them make them more vulnerable to theft or guesswork. In the proposed research, the researcher designed an algorithm that has the ability to perform registration or to access web applications safely. The researcher designed an algorithm in the proposed research, which has the ability to securely perform registration or access web applications. The proposed idea based on the notion of Zero-knowledge proof. A complex generation of random number initiated by proposed novel 6D-Hyper chaotic system. The bottom line is that both parties (web application, user), have a secret number. These two numbers used to do the process of registration without requiring a password. Results from the research showed the importance of the proposed method by which the keys were managed and distributed in a safe and effective way.

Corresponding Author:

Shatha J. Mohammed,
Department of CS, College of Science,
Mustansiriyah University, Baghdad, Iraq.
Email: shonash77@gmail.com

1. INTRODUCTION

We are all aware that developing and enforcing security based on risk assessment makes sense. Such an analysis would rely on the possibility of the threat being turned into an attack and its effect, if this happens. Although such an assessment can differ with respect to implementations and their meaning, a general study of the attacks points to certain patterns and directions.

The goal of organization-set password policies is to increase the security level of the used passwords via specification of different requirements applicable when the selection process and actual use. When users select and remotely use strong passwords, the password policies will help in protecting the the user account data and prevent malicious activities from unauthorized users which can cause network or service-wide compromise and harm the company further due to liability concerns. Without password user policies, users can select bad or easily guessable passwords and their accounts can be compromised vua dictionary attacks [1].

When implemented in a security environment, port knocking can provide an additional layer of server authentication, facilitate a defense-in - depth strategy, and mask the presence of services. Protecting against server-driven assaults is ideal, ranging from automatic scanning as part of assault chain identification to specifically target zero day exploitation. Port knocking solutions as a basic method for opening firewall ports have evolved and improved significantly. Many modern port knocking implementations have gained complexity layers from their predecessors in the process of eliminating unique vulnerabilities [2].

1.1. Theoretical background

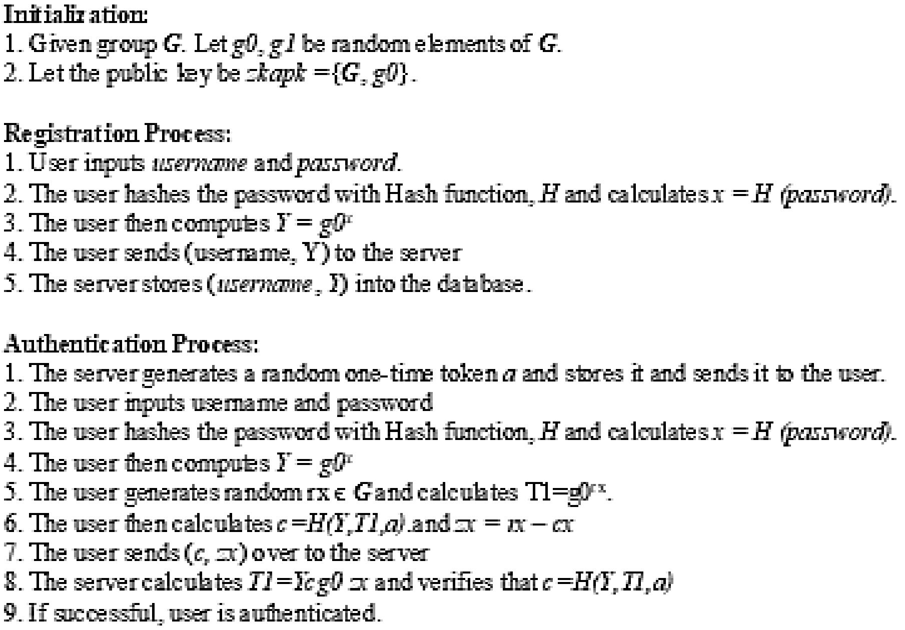
1.1.1. Zero-knowledge proof

Zero-knowledge protocols allow implementation of some basic cryptographic operations, such as identification, key exchange, etc without exposing any secret information during active conversation; it requires smaller computational effort compared to the use of some public key protocols. This protocol is attractive in embedded and smart cards applications [3]. As a popular concept in most cryptographic systems, Zero-Knowledge proof involves two parties identified as the prover (A) and the verifier (B). This technique requires the prover A to establish that he has a credential (say a credit card number) without necessarily having to reveal the exact number to the verifier B. A Zero-Knowledge Proof is required as an authentication system in this situation for the following reasons [4]:

- Completeness: if the statement is valid, the truthful verifier must be able to show that the statement is accurate to an impartial verifier at all times.
- Soundness: if the statement is incorrect, it is not possible to manipulate the result (with a very small chance) to the verifier that the statement is accurate.
- Zero-knowledge: the verifier does not know anything other than the fact that the statement is true if it is valid. No information will be released on the specifics of the document.

Algorithm (1), describe the Zero-Knowledge Proof that used in proposed idea. The following is a step-by-step procedure of the protocol [5]

Algorithm (1): Zero-Knowledge Proof Procedure of Protocol.



```
Initialization:
1. Given group $G$. Let $g0, g1$ be random elements of $G$.
2. Let the public key be $zkapk = \{G, g0\}$.

Registration Process:
1. User inputs username and password.
2. The user hashes the password with Hash function, $H$ and calculates $x = H$ (password).
3. The user then computes $Y = g0^x$
4. The user sends (username, Y) to the server
5. The server stores (username, Y) into the database.

Authentication Process:
1. The server generates a random one-time token $a$ and stores it and sends it to the user.
2. The user inputs username and password
3. The user hashes the password with Hash function, $H$ and calculates $x = H$ (password).
4. The user then computes $Y = g0^x$
5. The user generates random rx ϵ $G$ and calculates $T1=g0^{rx}$.
6. The user then calculates $c = H(Y,T1,a)$ and $zx = rx - cx$
7. The user sends $(c, zx)$ over to the server
8. The server calculates $T1 = Y^c g0^{zx}$ and verifies that $c = H(Y,T1,a)$
9. If successful, user is authenticated.
```

1.1.2. Chaotic system

Chaos can be described as follow: The property of a complex system whose action is so unpredictable as to appear random, owing to the high sensitivity to minor conditions changes. The formless matter that was supposed to have existed before the universe formed. The confusion and diffusion processes should be implemented by any cryptographic system according to Shannon's concept pro- posed [6, 7]. These processes match periodicity, a mixing property, and high sensitivity to the small variations in initial conditions or control parameters in chaotic systems [8, 9]. Therefore, the chaos phenomenon may be a prospective pseudo-random source, which is generally used in information security. Chaotic systems used extensively in many branches of science.

1.1.3. 6D hyper chaotic system

In this paper, we use a proposed novel 6D-Hyper Chaotic System. The novel six-dimensional autonomous system is obtained as follows:

$$
\begin{aligned}
\frac{\mathrm{dx}_1}{\mathrm{dt}} &= -a\,x_1 + b\,x_2 - x_5 + x_6\,\mathrm{Sin}(x_4) \\
\frac{\mathrm{dx}_2}{\mathrm{dt}} &= -c\,x_2 + d\,x_1 - \ e\,x_1\,x_3 - x_1\,\mathrm{Sin}(x_5) \\
\frac{\mathrm{dx}_3}{\mathrm{dt}} &= -f\,x_3 + x_1\,x_2 + x_4\,\mathrm{Sin}(x_1) \\
\frac{\mathrm{dx}_4}{\mathrm{dt}} &= -x_4 - x_2\,x_3 - g\,x_1\,\mathrm{Sin}(x_6) \\
\frac{\mathrm{dx}_5}{\mathrm{dt}} &= -x_5 - h\,x_3 + i\,x_3\,\mathrm{Sin}(x_2) \\
\frac{\mathrm{dx}_6}{\mathrm{dt}} &= -j\,x_6 - k\,x_3 x_4 + x_2 \mathrm{Sin}(x_3)
\end{aligned} \qquad (1)
$$

where x1, x2, x3, x4, x5, x6 and t □ □$^+$ called the states of system and a,b,c,d,e,f,g,h,i,j, and k are positive parameters of the system. The 6-Dimentional system (1) portrays a chaotic attractor upon chosing the values of the system parameters as follows:

a=10.2, b=12, c=5.1, d=30, e=2.5, f=2, g=5,h=0.5, i=10, j=17, and k=4.

We take the initial conditions as:

x1(0)=0.5 , x2(0)=2, x3(0)=1.5, x4(0)=6, x5(0)=0.4 and x6(0)=1.

According to the nonlinear dynamical theory, a quantitative measure approach of the sensitive dependence on the initial conditions is to calculate the Lyapunov exponent (LE) which is the average divergence or convergence rate of two nearby trajectories. Moreover, the 10 LEs of a nonlinear dynamical system as in System (1) with parameters a=10.2,b=12,c=5.1,d=30, e=2.5, f=2,g=5,h=0.5,i=10,j=17,and k=4. Results obtained as below:

L1= 4.72625,	L2= 1.06765,	L3= -1.26405,
L4= -4.89365,	L5= -14.9575	L6= -21.0403

Observably, the largest LE is positive, showing chaotic nature of the system. Being that $L1$ and L2 are a positive Lyapunov exponent, it is expected that the remaining 3 LEs are negative. Thus, the system is hyper-chaotic. The numerical simulation was performed using the MATHEMATICA program. This nonlinear system presents both complex & abundant chaotic dynamic behaviors; Figure 1 and 2 presents the strange attractors in 3D while the 2D representation of the strange attractors are depicted in Figure 3 and 4. Both Figures 1 and 3 showed the shape of the topology looking like a flying butterfly with flipping wings.

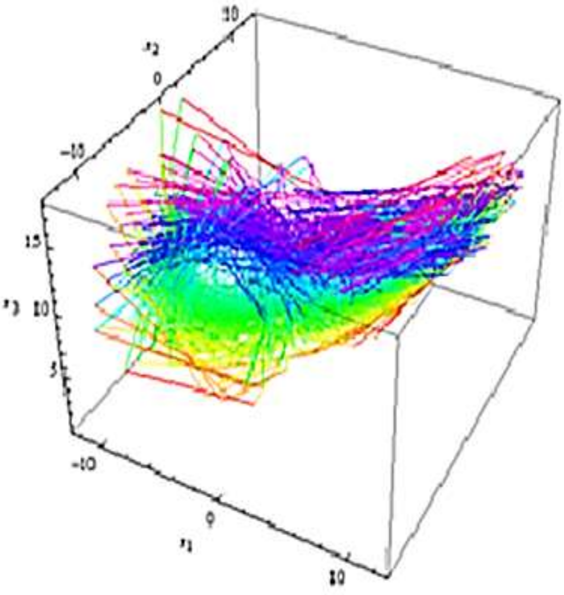


Figure 1. Chaotic attractors, three- dimensional view (x1-x2-x4)

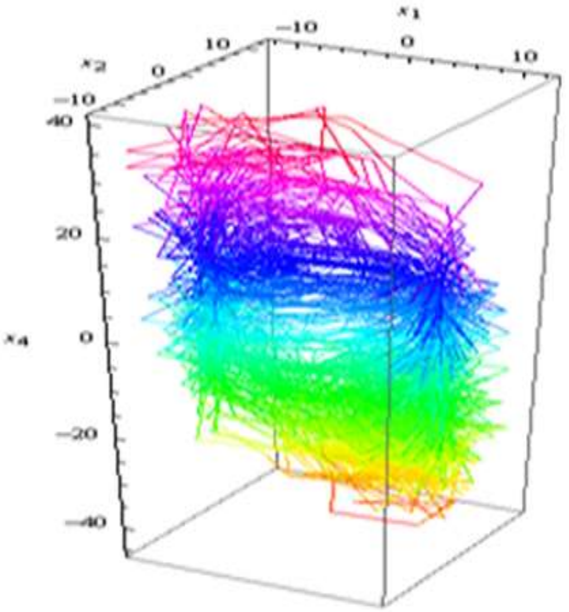


Figure 2. Chaotic attractors, three- dimensional view (x1-x2-x3)

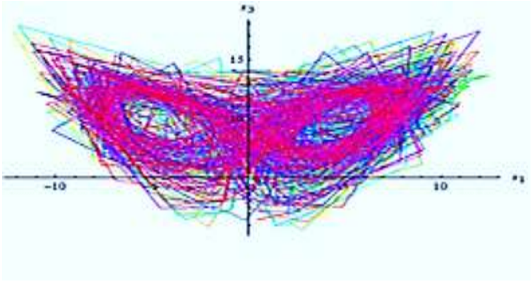


Figure 3. Chaotic attractors 2D, x3–x1 phase plane

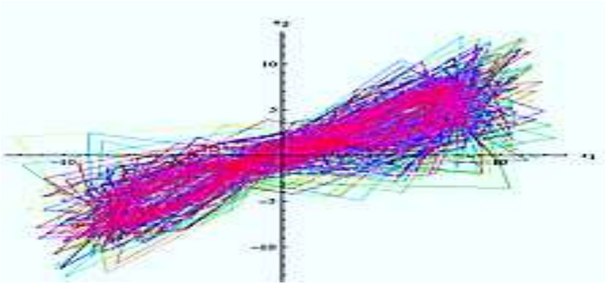


Figure 4. Chaotic attractors 2D, x2–x1 phase plane

2. WEB APPLICATION SECURITY

To ensure safe transaction and protected access to web-based sensitive resources, user authentication is a basic requirement. Whenever a web application provides authentication, both login and password details are sent to the user but in most instances, HTTP moves credentials from a client to a server. Most times, the credentials may not be stored in plaintext form on servers by some existing solutions for security reasons but sent to the servers during the authentication process in a readable form. Some other solution can rely on using the HTTP Digest Mode 2, but the issue with this approach is the chances of the server impersonating a third party with the request and this is a serious privacy-related issue. However, this issue is usually ignored by most non-commercial web application developers. Asymmetric cryptography communication protocols such as HTTPS are commonly used by developers for the development of commercial software, such as on-line banking and shopping software. This protocol provides a secure connection; hence, the credentials are still being sent. This problem is partly resolved with public key as the users are meant to provide either key pairs or digital certificates, both public and private. However, users are used to logging in and passwords that are easy to recall and convenient to use. Security of Web applications defined as the methods, principles and implementation used to avoid and identify security threats. Security can be understood as effective threat-free measure solution [10].

In a web application, the standard way to authenticate a user is to ask the user for a login and password. The username and password will then be sent directly to the server see Figure. 5 and the server will address the question. An HTTPS protocol used when protection is required. However, the passwords sent over Internet and servers can read them, even though the password is stored in a hashed and salted form. For instance, a user can often visit a website whose browser cannot verify the certificate. Typically, the browser allows users to accept the certificate though its verification has been unsuccessful.

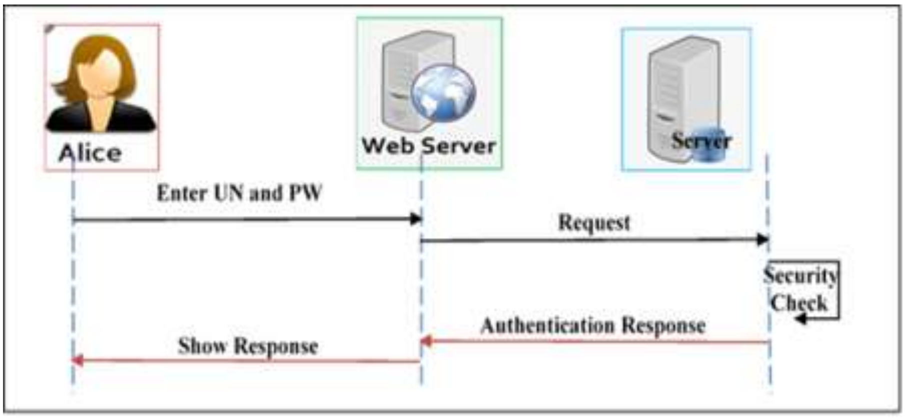


Figure 5. Classical way of authentication on the Web [10].

The open web application security project (OWASP) is a universal, non-profit association dedicated to security of web applications. One of OWASP's center standards is that their entire materials are uninhibitedly accessible and effectively open on their site, making it workable for anyone to improve security for their own web apps [11-16].

Below are OWASP Top 10 Web Application Security Risks [17-26]

1) Injection: This is encountered when unverified data is transmittd to a code interpreter in an input form or through other ways of data submission to a web application. It is referred to as an SQL injection attack.
2) Broken Authentication: Attackers can exploit vulnerabilities in authentication systems to gain access to legitimate user accounts and could have a chance of compromising the whole system from such compromised user account. For instance, an attacker may have access to a list that contains numerous known combinations of username/password obtained during a data breach and try to use some of the combinations on a login system in a bid to see if any one will work. To avoid authentication vulnerabilities, some strategies, such as 2-factor authentication (2FA) and limiting the number of repeated login attempts, are used.
3) Sensitive Data Exposure: Attackers can access that data and use it for harmful purposes. A common way attacker steal sensitive information is by using man-in-the-middle attack.
4) XML External Entities (XEE): This attack targets XML input-parsing web applications.
5) Broken Access Control: This gives attackers the chance to bypass the authorization step in order to perform tasks as if they are legitimate users.
6) Security Misconfiguration: This vulnerability is the commonest one in the list; it is encountered when using default configurations or when displaying excessively verbose errors.
7) Cross-Site Scripting: Attackers can be exploited this vulnerability to execute malicious JavaScript codes on the browser of a victim. For instance, the attacker could send the victim an email that seems to be coming from a trusted bank but with a web link to that website of the bank.
8) Insecure Deserialization: This attack mainly targets numerous web applications that perform data serialization and de-serialization.
9) Using Components with Known Vulnerabilities: Components such as libraries and frameworks are used by most of the modern web app developers.
10) Insufficient Logging and Monitoring: Many web applications are not taking enough steps to detect data breaches.OWASP recommends the implementation of loggingand monitoring by the web developers; they should also implement incident response plans to ensure they can detect attacks targeted at their applications.

3. METHODOLOGY AND ANALYSIS

Advances and growth of web application have led to an increase in design and security complexity. This paper proposes a novel authentication solution, which is a secure login and registration system, with high usability and stealth features to keep servers and services secret and safe. The proposed solution is stateless, requiring only the client to memorize a command, the IP of the server and the password chosen. The solution is transmitted as a method to protect servers from attacks ranging from port scans to day zero exploitation. Cryptographic hashes were created via chaotic systems, to function as a random for both client and server. The main idea depends on generating random numbers. In this side, researcher suggest a 6D-Hyper Chaotic System. Another contribution in this paper is achieve Authentication, this one of most important Top 10 risks that explained in OWASP report, this problem named authentication broken which solved using Zero-Knowledge Proof protocol with adaptation and modification suggested by researcher.

4. PROPOSED MODEL

Table 1 illustrate the general proposed model structure. There are two sides of the Client and Server model being introduced, each of them conducting different processes and services to complete proposed authentication method. A random number generator, based on the combination of proposed system. The generator produces a sequence consisting of 32-bit blocks for three initial seeds given. The treatment includes permutations and XOR operation on the lesser 32 bits of the elements obtained from chaotic system.

4.1. Initialization

A series of random numbers generated in a list format at this stage that can be used in any step involving random numbers, using chaos theory, the outputs of which are often complex decimal numbers.

4.2. Registration

There is a user that enters the username and password when first registers. The registration process shown in the proposal is split into two essential steps, the first stage being the initialization and the second stage being the registration. At initialization, generator uses the chaotic method as shown in the Figures 1-4 which generates a group of highly randomized numbers, these numbers are stored in a chaotic list, which will be used early in the registration step.

Server will be selected from these random numbers (g0) as the general random number for each client, this number will be known to both the client and the server. Stages of registration described in detail in Table 1. Now, in the hashing algorithm, the password is the entry to this algorithm, which could have been any size and length, output always fixed size, this password is padded to 512 bits after transforming it from ASCII code into binary format. 512 bits for blocks broken down to 16 words each block consists of 32 bits, the result of the hash algorithm is 128 bits, which is very secure since the original output data cannot be eversible. In this case, there is a certainty that the Server will never store the password. This is done by using zero knowledge protocol. It is a recent addition, which supports the power of the proposed research algorithm.

Table 1. General structure of proposed model of authentication.

Steps	Client Side	Server Side
Step#1	Initialization Step	
		1- Generate random numbers using proposed 6D-Chaiotic system section (2.3).
Step#2	Registration Step 1- Client request random value (g0) from server	
		1- Send random value g0 which choose randomly from List to client
	2- Client receive g0 from Server 1- Client enter HR_ID, Password and other Data 2- Compute X=hash(Password) by using MD5 3- Compute $Y=g0^X$ by using Fast Exponentiation	
	4- Client send HR_ID,Y,g0,Other data to server	2- Server receive HR_ID,Y,g0, other data and then store it in Main Database
Step#3	Login step	
	1- Generate random numbers using List.	1- Generate random numbers using List.
	2- Choose a private key from (List) and return it in (d) and calculate public (e) from (d) 3- Client enter user name and password 4- Send Public key (e) and username to server with Client request random value (a) and (g0) from server	
		2- Server receive public key(e),username and client request 3- Server Choose (a) as random value from List and g0 from Main database based on username 4-Server Calculate ae by encryption (a) based on public key : $ae=a^e$ 5- Send encrypted value (ae) and g0 to client
	5- Client receive ae and g0 6- using private key (d) to compute (a) $a= ae^d$ 7- Compute X=hash(Password) by using MD5 8- Compute $Y=g0^X$ by using Fast Exponentiation 9- Choose plaintext (m) randomly from List 10- Calculate T1 using $T1=m^d$ 11- Calculate C by Hash three value are Y,m and a therefore C=hash(Y,m,a) 12- Send two values to server T1 and C	
		6- Server receive T1,C from Client 7- Server calculate (m) By using $m= T1^e$ 8- Return Y from database base on username 9- Server compute newC by newC=hash(Y,m,a) 10- Compare (C,newC) , if it equal then user is authenticated otherwise not-authenticated 11- Server send comparison result
Step#4	Authentication Successes	

4.3. Authentication

Every user has an account created for him at the registration stage. In this plan, the login algorithm has two stages, first initialization, where random keys are generated at this point using a chaotic system as previously shown, and second authentication method to validate user identity, where authentication is primarily at each user login to the website. In authentication, the (a) variable was selected by server for each new session to make it impossible to detect in the authentication process from the intruder, and (a) item was stored in a hidden buffer at the time of the session to encrypt in the next steps to prevent it from being revealed to the public interest.Server encrypts (a) to produce (ae) using the client's public key and sends the encrypted value to the client to be decrypted using the private key, in which case the client selects the random number (m) from the Generated List by proposed chaotic system, and encrypts it using RSA with (d) as the key to obtain (T1) and then uses the three values a, m and Y to generate the value (c) using the hash algorithm. Finally, the server still has the three (Y, m, a) from which (c) is collected from the client to equate it with (c), to test whether it is authenticated or not.

5. RESULTS AND DISCUSSIONS

Proposed framework applied to Web application for e-learning. This e-learning web application has been designed with ASP.Net and contains many services that teachers as well as students require. The proposed system works to secure the most critical stage of a framework that should be more authentic and secure for users to log in or register in the system. Then introduced a protocol, as described earlier in Table 1. Researcher recommended that a ZKP protocol with RSA algorithm and digital signature principles be used to protect the non-disclosure or use of passwords that are vulnerable to theft or speculation. The process of producing random numbers was further complicated by the use of chaos theory, specifically the proposed 6D Chaotic system algorithm. The results of the proposed research showed the effectiveness of the approach used, as well as the achievement of the protective elements established using CIA, which is an important basis for securing web-wide sites and applications.

We conducted a large-scale analysis of the password meter, finding the meter had an effect on user behavior and safety. Meters have caused users to create more passwords. Nevertheless, unless the meter rated passwords stringently, the resistance of the resulting passwords to password cracking attacks is minimal. The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. NIST applied to the proposed system. Testing results as illustrated in Table 2.

Table 2. NIST testing results of proposed model

Index	Test	P-value	Result
1	Frequency	0.9105	Pass
2	Block frequency	0.4681	Pass
3	Runs	0.2049	Pass
4	Longest-run-of-ones	0.364	Pass
5	Binary matrix rank	0.2602	Pass
6	DFT(Spectral)	0.6712	Pass
7	Non overlapping template matching	0.8917	Pass
8	Overlapping template matching	0.361	Pass
9	Maurer's universal statistical	0.9762	Pass
10	Linear complexity	0.9657	Pass
11	Serial1	0.4374	Pass
12	Approximation entropy	0.1602	Pass
13	Cumulative sums	0.9775	Pass
14	Random excursion	0.9678	pass
15	Random Excursions Variant	0.9128	Pass

6. CONCLUSION

The random numbers that are generated using chaotic are very safe. It gives the system, because each number is unpredictable, a very high randomization that gives robustness. Thus, attackers and any users cannot obtain the passwords of members by using the new authentication method where it was the combination of Zero Knowledge method with proposed chaotic system and RSA algorithm. Many keys used in the framework being proposed are complex and strong keys. The main reason for this is the proposed chaotic system, a new addition to the process of generating random numbers that go into RSA algorithm work. The proposed method for the key generation examined using NIST 15 testing. That demonstrated a rather important convergence to the organization's verified ideal results**.**

REFERENCES

[1] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. "How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation", In USENIX Security'12, pages 5–5. USENIX Association, 2012.

[2] Major, W., Buchanan, W.J. & Ahmad, J., "An authentication protocol based on chaos and zero knowledge proof", *Nonlinear Dyn 99*, pp. 3065–3087 (2020). https://doi.org/10.1007/s11071-020-05463-3

[3] Hannu A. Aronsson, "Zero Knowledge Protocols and Small Systems", Department of Computer Science, Helsinki University of Technology, 2007.

[4] Lum Jia Jun, Brandon., *"Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk*)", The Python Papers Monograph 2: 9 Proceedings PyCon Asia-Pacific, 2010.

[5] Abeer Tariq, "SMSCC: Smarter and More Secure Credit Card Using Neural Networks in Zero Knowledge Protocol", Al-Rafidain University College For Sciences , ISSN: 16816870 Year: 2014 Issue: 34 Pages: 227-243.

[6] Aleksandra V. Tutueva and others, "Adaptive chaotic maps and their application to pseudo-random numbers generation", *Chaos, Solitons & Fractals Journal*, vol. 133, April 2020. https://doi.org/10.1016/j.chaos.2020.109615

[7] Shannon CE., "Communication theory of secrecy systems", Bell Syst Tech J 1949; 28(4):656–715.

[8] Sadiq A. Mehdi and Ashwaq A. Kadhim, "Design and Analysis of a Novel Five-Dimensional Hyper-Chaotic System", Part B: *Applications An International Journal of Research and Surveys*, vol. 11, no. 1, January 2020

[9] Rageed Hussein AL-Hashemy and Sadiq A. Mehdi , "A new Algorithm Based on Magic Square and a Novel Chaotic System for Image Encryption", *Journal of Intelligent Systems*, ISSN: 0334-1860, de Gruyter GmbH, Berlin/Boston. 29(1)m pp. 1202–1215, 2020.

[10] Sławomir Grzonkowski and others, *"Extending Web Applications with a Lightweight Zero Knowledge Proof Authentication",* CSTST '08: Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology. pp. 65-70, October 2008. https://doi.org/10.1145/1456223.1456241.

[11] Sandeep Kumar, Renuka Mahajan, Naresh Kumar, Sunil Kumar Khatri, *"A Study on Web Application Security and Detecting Security Vulnerabilities",* 6th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), IEEE Xplore: 23 April 2018, DOI: 10.1109/ICRITO.2017.8342469, Noida, India.

[12] Abdalla Wasef Marashdih and Zarul Fitri Zaaba, "Cross Site Scripting: Detection Approaches in Web Application", *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 7, no. 10, 2016.

[13] OWASP Foundation, "OWASP Top 10 -2017, The Ten Most Critical Web Application Security Risks", 2017.

[14] Je Sen Teh, Moatsum Alawida., "You Cheng Sii,Implementation and practical problems of chaos-based cryptography revisited," *Journal of Information Security and Applications*, vol. 50, 2020.

[15] Nashreen Nesa, Tania Ghosh, Indrajit Banerjee., "Design of a chaos-based encryption scheme for sensor data using novel logarithmic chaotic map," *Journal of Information Security and Applications*, vol. 47, 2019.

[16] Gao T, Chen Z. A., "New image encryption algorithm based on hyper-chaos". *Physics Letters A*. 372(4): pp. 394-400. 2008.

[17] Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H., "A chaos-based symmetric image encryption scheme using a bit-level permutation." *Information Sciences*, 181(6), pp. 1171-1186, 2011.

[18] Fu, C., Zhang, Z. C., Chen, Y., & Wang, X. W., *"An improved chaos-based image encryption scheme".* In International Conference on Computational Science. pp. 575-582, 2007. Springer, Berlin, Heidelberg.

[19] M. A. Mohammed, I. A. Mohammed, R. A. Hasan, N. Ţăpuş, A. H. Ali, and O. A. Hammood, *"Green Energy Sources: Issues and Challenges,"* in 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), pp. 1-8, 2019.

[20] H. R. Ibraheem, Z. F. Hussain, S. M. Ali, M. Aljanabi, M. A. Mohammed, and T. Sutikno, "A new model for large dataset dimensionality reduction based on teaching learning-based optimization and logistic regression," *Telkomnika*, vol. 18, 2020.

[21] M. A. Mohammed and N. ŢĂPUŞ, "A Novel Approach of Reducing Energy Consumption by Utilizing Enthalpy in Mobile Cloud Computing," *Studies in Informatics and Control*, vol. 26, pp. 425-434, 2017.

[22] N. Q. Mohammed, M. S. Ahmed, M. A. Mohammed, O. A. Hammood, H. A. N. Alshara, and A. A. Kamil, "*Comparative Analysis between Solar and Wind Turbine Energy Sources in IoT Based on Economical and Efficiency Considerations,"* in 2019 22nd International Conference on Control Systems and Computer Science (CSCS), pp. 448-452, 2019.

[23] M. A. A. Royida A. Ibrahem Alhayali, Yasmin Makki Mohialden, Ahmed H. Ali, *"Efficient method for breast cancer classification based on ensemble hoffeding tree and naïve Bayes,"* Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, pp. 1074-1080, 2020.

[24] Z. H. Salih, G. T. Hasan, and M. A. Mohammed, *"Investigate and analyze the levels of electromagnetic radiations emitted from underground power cables extended in modern cities,"* in 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2017.

[25] Z. H. Salih, G. T. Hasan, M. A. Mohammed, M. A. S. Klib, A. H. Ali, and R. A. Ibrahim, *"Study the Effect of Integrating the Solar Energy Source on Stability of Electrical Distribution System,"* in 2019 22nd International Conference on Control Systems and Computer Science (CSCS), pp. 443-447, 2019.

[26] N. D. Zaki, N. Y. Hashim, Y. M. Mohialden, M. A. Mohammed, T. Sutikno, and A. H. Ali, "A real-time big data sentiment analysis for iraqi tweets using spark streaming," *Bulletin of Electrical Engineering and Informatics*, vol. 9, pp. 1411-1419, 2020.