iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Design and Development of Two Factor Authentication System for E-Services Using DNA and Asymmetric Cryptography

Priyanka B J[1] , Nalinakshi B. G[2] , Dr. D Jayaramaih[3]
[1]M.Tech, [2]Associate professor, [3]Prof and HOD, Dept. of ISE
The Oxford College of Engineering Karnataka, India.

Abstract: ***DNA cryptography is a new technology that uses biological concepts for encryption and decryption of data. There is a lot of growth in the field of mobile devices using for e-transaction using internet and wireless network. So To achieve secure communication and mutual authentication; two schemes are constructed from DNA hybridization and DNA digital coding techniques. Two factors authentication uses the OTP (One Time Password) and SAC (Server Authentication Code) for the better security. This paper presents a secure and efficient authentication mechanism for mobile e-banking services using RSA encryption and DNA cryptography. The comparative analysis between these schemes shows that DNA cryptography based authentication provides more security than the RSA based authentication in terms of computational complexity.***
Keywords: DNA cryptography, DNA computing, Challenge-Response Authentication, Mobile security, Attacks.

I. INTRODUCTION

There are wide types of electronic services receiving smart phones have been growing rapidly. Using wireless technology the mobile phones started using e-service applications. The mobile phone users can access the internet through wireless communication in the field of wireless networks. All the mobile phone users are concerned about the security issues to use the e-services through the wireless internet. In order to achieve secured e-services, the four security functions such as integrity, confidentiality, non-repudiation and user authentication must be provided in wireless internet as in wired internet. By using any technology or applications to the wireless technology the security should be comparable with the wired technology.

Secure communication is nothing but a secure authentication is done to secure user and secret session key is established for confidentiality. As the methods and schemes grows for the cryptography, in parallel the same security schemes should be developed for the user authentication and key agreement. At the beginning of the cryptography the security is based on the passwords. The very first key agreement schema has been implemented by the Diffie and Helmen during the introduction of asymmetric key in the cryptography and since it does not provide secured authentication and vulnerable to attacks. Lamport has designed and proposed the very first authentication scheme based on the passwords. Most of these schemas depends public key cryptography. To overcome the drawbacks the hash function came into existence. By the Adleman's pioneering work DNA computing came into existing. By the design of his

DNA algorithm for solving the Hamiltonian problem, Adleman set the foundation for the research in the field of bio computing. Many researches thought after the results Adleman's experiments, because DNA's parallelism and large information storage capacity DNA computing can used in the field of cryptography to achieve the strong authentication. DNA cryptography increases the complexity of the problem by increasing its size so that an attacker requires huge number resources and efforts to break

This paper includes design and development of two protocol based on public key cryptography and DNA cryptography. By using the advantages of RSA algorithm and DNA techniques the problems in the web authentication scheme can be solved. Security analysis is done to prove that DNA based authentication scheme provides higher security than the public based scheme in terms of computational complexity and number attacks they overcome. Both the protocols two factors authentication schemes is done using OTP and SAC value, which are computed with different mathematical functions and DNA conversions.

II. LITERATURE SURVEY

Includes various types of authentication schemes, brief overview of the DNA cryptography and different techniques used in the DNA cryptography.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A. Authentication Scheme

There are many ways to provide the credentials for the authentication. The most commonly used method but not more secured is password authentication. Now a day the competitive e-commerce demands for methods that provides more protection when network resources includes highly sensitive data [9]. Smart cards and biometric authentication types provide this extra protection.

1) *Computer Recognition System:* it requires the installation of some small authentication software in the system. In the authentication process this can be verified as second authentication factor.
2) *Password Authentication: is* the most commonly used authentication form. Here user provides the username with password. The username are mostly a string of characters, numbers so it is vulnerable to guessing attack. Password may be easy to guess. By using digests for authentication the risk of eavesdropping can be minimised.
3) *Single Factor Authentication:* is a process where single credential is used to secure the critical data unauthorized access to system.
4) *Two factor authentication:* is a process where two credentials are used secure the unauthorized access to system and critical data.
5) *One Time Password (OTP):* OTP authentication is a method to reduce the possibilities of compromised user credentials using login passwords that are only valid once. If an attacker is successful in sniffing the password that a user has used to enter in a site, it is of no use because the password is no longer valid. Moreover, it is highly difficult to predict the next password based on the previous one. Each time the OTP generated by the password-generating token are unique [3]. The function that generates such passwords must be non-invertible. There are three types of schemes to generate one-time passwords:

Based on time, such as Secure Id. Time-synchronization is required between the authentication server and the client providing the password. Based on a challenge (e.g. a random number chosen by the authentication server or transaction details) and a counter. Based on some internal data (e.g. the previous password) or counter (e.g. systems based on hash chains, such as S-Key [10])
Authentication is the very big issue now a day; the new protocol is designed for the purpose of achieving the high secured authentication using the public key encryption and DNA technology.

B. DNA Cryptography

With the lot of advances in the field of DNA computing the new technology has come into existence called as DNA cryptography which is far better than the traditional cryptography in point of providing authentication, security, integrity, storage capacity etc. In the DNA cryptography the encryption is done by converting the human readable form into bases of DNA strands, which creates a strong base for the authentication and digital signature. There are some techniques such a DNA digital coding and DNA indexing used for hiding the data. DNA indexing and DNA digital coding techniques are the most important for DNA Cryptography, a brief description about these two techniques are discussed in the previous chapter. The other few DNA Encryption Techniques are as described below:

C. DNA Digital Coding

DNA digital coding is the important technique used for encryption and decryption process which is based on the mapping of base pairs. DNA coding is done based on nucleotide bases A, C, T, G. such that A always makes pair with T and C always makes pair with G of two strands. In the mathematical point of view it is possible to produce 24 patterns but according to DNA complementary rules only 8 patterns are identified correctly such as 0123/CTAG, 0123/CATG, 0123/GTAC, 0123/GATC, 0123/TCGA, 0123/TGCA, 0123/ACGT, 0123/AGCT and among these 8 patterns, 0123/CTAG perfectly reflects the biological characteristics of four nucleotide bases.

Table1: DNA digital coding pattern [6]

Digital coding	DNA code
00(0)	A
01(1)	T
10(2)	C
11(3)	G

III. CURRENT PRACTICES

There are many ways to provide the credentials for the authentication. The most commonly used method but not more secured is password authentication. Now a day the competitive e-commerce demands for methods that provides more protection when network resources includes highly sensitive data [9]. Smart cards and biometric authentication types provide this extra protection.

There are some OTP solutions based on a mobile phone. In [14, 15] a multichannel communication is used (Internet and GSM) in order to improve the security of the authentication scheme. In [13] a user logs in the web site using a username and a password. Then, a one-time password is sent via SMS to his mobile, and the user enters this data in the web authentication form. If it is correctly verified, the user is authenticated into the application. In this system the mobile is used as a mere point of reception, not as a hardware token that stores and computes keys.

On the other hand, In [14] what is sent though the GSM channel is a challenge. The mobile computes a one-time password using this challenge and sends it to his computer through a bluetooth connection. Finally, the password is forwarded to the server. The main trouble of these two schemes that rely on SMS messages to perform the authentication is that the session establishment between the user and the server is slow because SMS messages are not real-time. Thus, the system is not practical. On the other hand, users may want to connect to their Internet bank accounts from places in which there is no cellular connectivity (in some sensitive environments GSM signals are blocked), and these models do not allow it.

Other OTP solutions [15, 16] deal with a password generation in the mobile using as input a server challenge sent through the Internet connection. Once in the PC, the challenge is transferred to the mobile using a bluetooth channel. The problem is that bluetooth is usually not available from public access computers. Besides, it presents some relevant vulnerabilities and threats [17, 18] -most of which due to faulty implementations- that jeopardize the system.

Some other OTP mobile schemes focus on the speed of the process and base the generation of the one-time password on a time factor (no server challenge is needed). This is the case of the Free Auth Project [17]. The inconvenient of using this approach in a mobile context is the required time synchronization between the mobile and the server. Users roughly configure the clock of the mobile phone when they travel, and they are not very much concerned on setting the correct time zone. Hence, protocols based on absolute time are not feasible.

The MP-Auth scheme [18] uses the mobile as a secure device to store keys and encrypt passwords for web authentication. It is a one factor authentication mechanism that safeguards passwords from keyloggers, phishing attacks and pharming. Nevertheless, if an attacker learns a user password he can impersonate that user.

IV. PROPOSED SCHEME

The proposed scheme provides the secure authentication to the e-services. Both Asymmetric and DNA-OTP protocol follows same architecture for the communication.

A. DNA-OTP Scheme

The DNA-OTP scheme comprises of web server, a browser. Data transmission is very simple between mobile phone and client PC, so it does not require any communication channel like Bluetooth, it can entered by using keypad. The DNA-OTP scheme consists of three phases those are registration phase, authentication phase, transaction phase. In the registration phase the server sends the initialization key in DNA form to user who is interested in registration. These initialization keys are stored in the mobile phones for future authentication. After successful registration the user can access to the web services through the second phase that is authentiation phase.

In the authentication phase the user sends his ID to the server, which computes the challenge in DNA sequence using DNA digital coding, replies with the challenge to user. The user computes the DOTP using challenge and other parameters and sends to the server. Server verifies the freshness of the submitted DOTP and determines whether the user is accepted or not. If the user is accepted the server will send the DSAC to the user. The user compares the received DSAC value with one he has computed using mobile phone. Once the DSAC values matches the transaction phase starts.

B. Asymmetric OTP Scheme

This scheme also includes three phases such as registration phase, authentication phase and transaction phase. In this scheme the public key encryption is used to generate the two factors required for the authentication. In the registration phase user provides the details to get register to the application service. Once the service is granted, server replies with the initialization key. Both user and server store their details in the DB. In authentication phase user provides username and password to gain access to the application.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Server replies with CH value if the login is successful. The client application computes OTP using RSA algorithm and enters the computed OTP value in the web site. Server verifies the received OTP if the value matches then first step of authentication is successful and displays SAC1 value. The user manually compares the both the values if matches then transaction phase starts. In the transaction phase the server sends the transaction ID to client and client generate the transaction authentication code and sends to the server and if the TAC is correct then actual transaction money takes place.

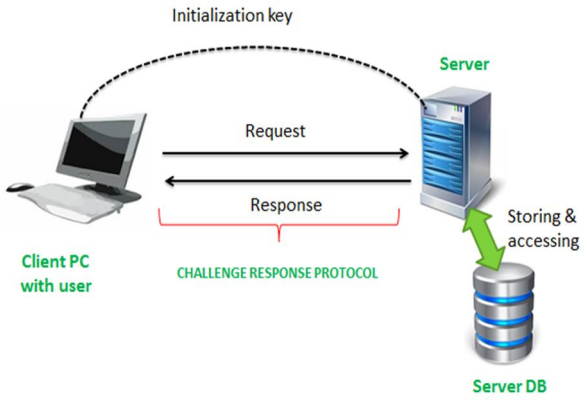


Figure2: System architecture.

V. SYSTEM DESIGN

The Figure3 shows the sequence diagram of the DNA-OTP deals with all three phases of the protocol, in registration phase the subscribed user sends his credential to register for the application. One the server receives the details of the user he generates and sends the DK0 that is initialisation key along with user id and server id. The user upon receiving the DK0 and other details, the user stores it in his mobile database by creating separate database for this server. At the same time the server creates database with user id. Server maintains the separate database for each individual user.

In the authentication phase comes after the registration phase, in this phase user sends the UID to server and server generates the DNA based DCH using random DNA sequence generator. User upon receiving the channel computes the temporary key by using the DCH and DK0. First he takes the hash of DCH using SHA 2 and resultant value is XOR with the DK0. Since DNA-OTP is two factors authentication schema so authentication is done in two steps using two generated secured values such as DOTP and DSAC.

The user and server both computes the values of the DOTP and DSAC values using the details stored in their data base. The user sends the DOTP to server and verifies whether the OTP computed by his is matches with this or not: if matches server will send the DSAC1 value to the user if not authentication fails at first step. After the success of first step authentication server sends the DSAC1 to user and user compares with his own generated DSAC value if matches then second step of authentication are successful if not authentication fails. Once the user authenticated successfully in both the steps the protocol enters to transaction phase. Here the server generates the DTID value and sends to user. The user upon receiving the DTID value he computes the DTA and sends to server, the server will verify the received DTA.

VI. COMPARATIVE SECURITY ANALYSES

In the asymmetric OTP there is a complexity in the key creation. RSA algorithm is limited to the prime numbers hence efficiency of generating primes are relatively low and difficult to generate secret one. The security of the RSA algorithm depends on the factoring the large prime numbers. The security can be threatened with the algorithm that decomposes a large number. The encryption and decryption needs a lot of calculation and speed of execution is slow and increases the time complexity. This scheme is vulnerable to the impersonation, even is users private keys are not available. The drawbacks of the asymmetric encryption scheme are overcome by DNA-OTP scheme.

The DNA–OTP scheme is developed using symmetric encryption, OTP, SAC and DNA hybridization to reduce the time complexity (0(n)). Time complexity of the encryption and decryption is increased in DNA algorithm because lot data conversions takes place while generating key value i.e. from normal text to ASCII then ASCII to binary and then binary to DNA sequence. To provide hybrid security in the authentication for e-banking DNA cryptography is combined with the traditional cryptography.

VII. EXPERIMENTS AND RESULTS

This chapter involves the average time taken by the RSA and DNA algorithm to encrypt and decrypt the file size of 2MB using different key size. In the following graph the decryption take taken by the DNA algorithm is more compare to RSA algorithm. From security point of view the algorithm which has higher decryption time lower transmission time is said to be highly secured. The DNA algorithm provides the higher complexity in generating the key values for the authentication and involves lot of data conversion for encrypting and decrypting the text file.

Table2: Values for the above graphs

Key size(bits)	RSA algorithm		DNA algorithm	
	Encryption time (ms)	Decryption time (ms)	Encryption time (ms)	Decryption time (ms)
512	110	215	190	230
768	175	281	255	295
1024	251	348	300	375
1280	328	413	386	455
1536	404	479	425	570
1792	479	546	518	618
2048	552	611	585	699

Table3: Transmission time taken by the RSA and DNA-OTP schemes.

Transmission time (ms)		
	RSA algorithm	DNA algorithm
512	3315	3229.85
768	3320	3233.8
1024	3326	3239.85
1280	3308	3222.8
1536	3317	3235
1792	3322	3240.34
2048	3340	3250

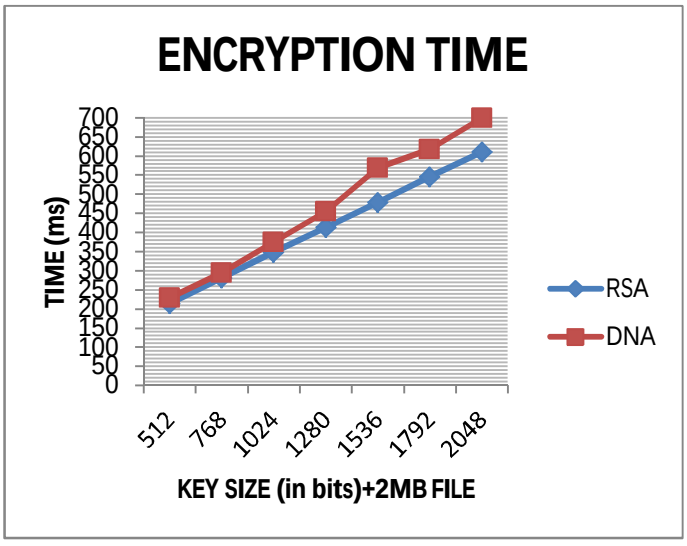


Figure4: Encryption time of DNA and RSA algorithm.

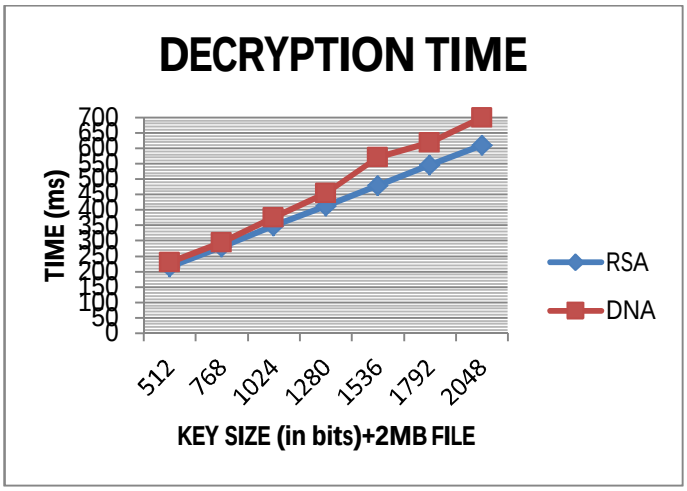


Figure5: Decryption time for DNA and RSA algorithm.

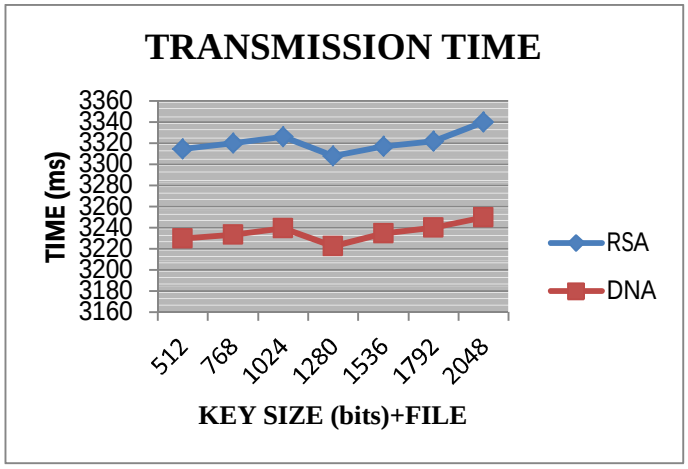


Figure6: Transmission taken by RSA and DNA algorithm.

$$\textit{The average encryption time taken by the RSA algorithm} = \frac{(\textit{Total taken to encrypt})}{(\textit{Total number of keys})}$$

$$\frac{(100 + 175 + 251 + 328 + 404 + 479 + 552)ms}{7} = \frac{2289ms}{7} = 327ms$$

$$\textit{The average encryption time taken by the DNA algorithm} = \frac{(\textit{Total taken to encrypt})}{(\textit{Total number of keys})}$$

$$\frac{(215 + 281 + 348 + 413 + 479 + 546 + 611)ms}{7} = \frac{2893ms}{7} = 413.28ms$$

$$\textit{The average decryption time taken by the RSA algorithm} = \frac{(\textit{Total taken to encrypt})}{(\textit{Total number of keys})}$$

$$\frac{(190 + 255 + 300 + 386 + 425 + 518 + 585)ms}{7} = \frac{2659ms}{7} = 379.85ms$$

$$\textit{The average encryption time taken by the DNA algorithm} = \frac{(\textit{Total taken to encrypt})}{(\textit{Total number of keys})}$$

$$\frac{(230 + 295 + 375 + 455 + 570 + 618 + 699)ms}{7} = \frac{3232ms}{7} = 461.71ms$$

From the above calculations the DNA algorithm takes 86.28 ms more than the RSA algorithm to encrypt the 2MB, 81.15ms more time than RSA algorithm to decrypt the and 0.08156 sec less transmission time than RSA algorithm when the different key size is used.

VIII. CONCLUSION

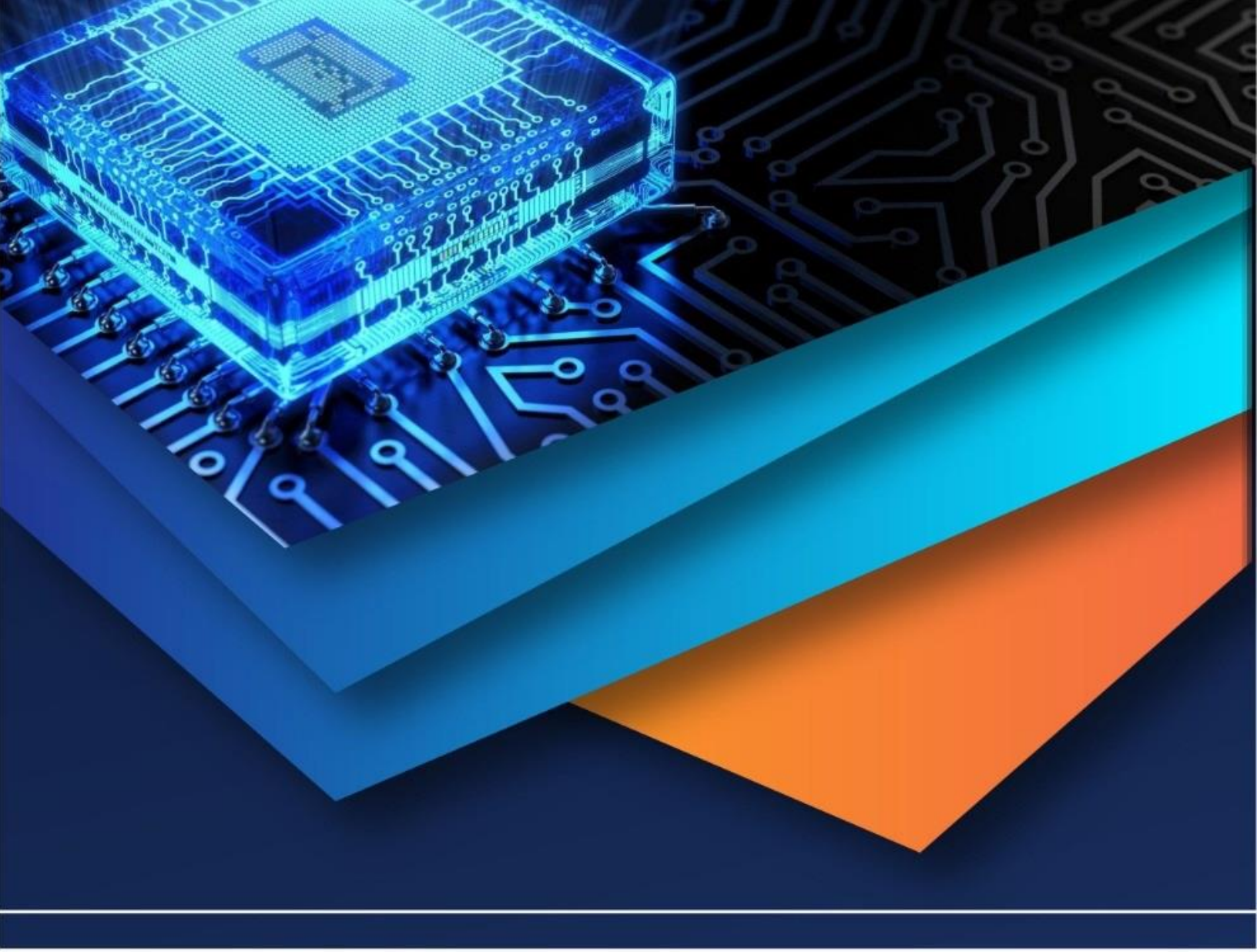
Current days e-services are very importance in many applications such as e-shopping, e- banking, e- ticket etc. but authentication is the main concern in all these applications. The aim of the protocol is to achieve the double layer authentication. One for authenticating the user with his ID and another is for authentication the server with his ID. The proposed protocol is providing the two step authentication with two different factors such as DNA-OTP and DSAC. The reason for the DNA technology for this protocol is because of its high computational power and unbreakable cipher text. An authentication done using RSA algorithm is less secured than the DNA based authentication in terms of complexity involved in logical computation, data conversions and matrix form involved in the DNA algorithm reduces time complexity of encryption and decryption.

IX. FUTURE WORK

In future, the designed protocol will be developed and implemented for real time application in any smart phone. This protocol will be implemented in the cloud for the purpose of storing the user details and focuses mainly on reducing possible attacks on it.

REFERENCES

[1] He, Debiao, et al. "One-to-many authentication for access control in mobile pay-TV systems." Science China Information Sciences 59.5 (2016): 052108.
[2] Misbahuddin, S. C. S, M. & Hashim, N. P. (2014). DNA for information security: A Survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology. International Conference on Computer and Communications Technologies. 11 – 13 Dec, Hyderabad
[3] R. R. Sinden, International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 12, December 2016
[4] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, 201
[5] Al-Qayedi, A., Adi, W., Zahro, A., Mabrouk, A.: Combined web/mobile authentication for secure web access control. IEEE Wireless Communications and Networking Conference (WCNC) 2 (March 2014) 677–68
[6] Javheri, S. & Kulkarni, R. (2014). Secure Data communication and Cryptography based on DNA based Message Encoding. International Journal of Computer Applications, 98(16), 360-363.
[7] C. Chou, K. Tsai, C. Lu. "Two ID-based authenticated schemes with key agreement for mobile environments". J Super comput 66:973-988, (2013)
[8] Cheswick, W.R., Bellovin, S.M., Rubin, A.D.: Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (2013)
[9] D. Wang, C. Ma. "Cryptanalysis of a remote user authentication scheme for mobile client C server environment based on ECC". Information Fusion 14, 498503, (2013)
[10] Yunpeng Zhang and Liu He Bochen Fu. Research on DNA Cryptography, Applied Cryptography 2012
[11] A. Atito , A. Khalifa , S. Z. Rida, DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques(2011
[12] Hakami, H. A., Chaczko, Z. & Kale, A. (2015). Review of Big Data Storage Based on DNA Computing, Asia-Pacific Conference on. IEEE Computer Aided System Engineering (APCASE), 14-16 July, Educador, 113-117 [10] Hornweder, K. S. V. (2011)
[13] An Overview of Techniques and Applications of DNA Nanotechnology, Technical Report UT-CS-11-682, (2011)
[14] Iqbal, Z.: Secure mobile one time passwords for web services (master of science thesis). Technical report, Royal Institute of Technology (May 2011)
[15] Hallsteinsen, S., Jorstad, I., Thanh, D.V.: Using the mobile phone as a security token for unified authentication. In: Proc. of the International Conference on Systems and Networks Communications (ICSNC), Washington, DC, USA, IEEE Computer Society (2011).
[16] Me, G., Pirro, D., Sarrecchia, R.: A mobile based approach to strong authentication on web. In: Proc. of the International Multi-Conference on Computing in the Global Information Technology (ICCGI), Washington, DC, USA, IEEE Computer Society (2011) 67
[17] Hager, C., Midkiff, S.: Demonstrating vulnerabilities in bluetooth security. Global Telecommunications Conference. IEEE GLOBECOM 3 (Dec. 2003) 1420–1424 16. Insight Consulting: How can bluetooth services and devices be effectively secured? Computer Fraud & Security (1) (Jan. 2010) 4–7
[18] FreeAuth Project: The freeauth. http://www.freeauth.org [Online; accessed on 10/2010].
[19] Mannan, M., van Oorschot, P.C.: Using a personal device to strengthen password authentication from an untrusted computer. In: Financial Cryptography (LNCS). Volume 4886. (2010) 88–103.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY