Volume 8, No. 5, May-June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Review on DNA Computing based Authentication Techniques

Er. Simranpreet Kaur
M.Tech Scholar
Department of Computer Science & Engineering,
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India

Er.Varinder Kaur Attri
Assistant Professor
Department of Computer Science & Engineering,
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India

Abstract: Within the age of the Internet, protecting our data has turn out to be simply as critical as shielding our belongings. Information safety is the exercise of protecting both bodily and digital statistics from destruction or unauthorized get entry to. Numerous strategies have been proposed to preserve safety of statistics so that best the authenticated people have to be able to acquire the message sent through the sender. DNA is a new method evolved for facts protection. It has many advantages over traditional methods along with low electricity consumption, excessive processing pace, lesser time intake and lesser computational overhead. This paper discusses diverse DNA based totally authentication techniques, cryptographic algorithms and their advantages and obstacles.

Keywords: DNA computing, Authentication and DNA Cryptography

1. INTRODUCTION

Modern research has countered DNA as a moderate for serious computation and for ultra-compact data storage. DNA cryptography is a whole new created cryptographic discipline turn out with the examination of DNA processing [1][2], wherein DNA is used as facts service and the cutting-edge biological automation is used as processing tool. The large parallelism and awesome records frequency inbuilt in DNA molecules are analyzed for cryptographic principles consisting of encryption, authentication, signature, and so forth. The most efficient key utility today is DNA-primarily based molecular cryptography structures. DNA processing offers a parallel computing facility with molecular stage, presenting a hearth-new information structure and intelligent technique, providing threats to standard information protection era. Studies on this area might also sooner or later result in the start of latest computers, new statistics garage systems and new cryptography structures, on the way to trigger a new facts revolution [3].

1.1 DNA Computing

The inspiration of understanding Deoxyribonucleic acid (DNA) evaluation needs knowledge of the primary additives of DNA. DNA is the genetic element obtained in maximum organisms, inclusive of humans. The principle function of DNA molecules is storing the information for long-period of time [4]. The data in DNA is saved as a rule produced from four compound bases: adenine (A), thiamine (T), cytosine (C), and guanine (G). Every base is likewise mounted on a sugar molecule and a phosphate molecule. The order, or series, of the bases is responsible for making male or female DNA different and decides the data to be had for making and keeping an organism, comparable to the manner in which words of the alphabet occur in a sure order to make words and sentences. The combination of a base, sugar, and phosphate are known as a nucleotide. Nucleotides are organized in two lengthy strands that produce a spiral known as a double helix [4]. Human DNA includes approximately 3 thousand bases, and over 98 % of these bases are similar in every person.

A computation may be idea of as the accomplishment of an algorithm, which itself can be referred to as a detailed technique of properly-determined commands that get some input, execute it, and produce a output. In DNA processing, data is displayed by the use of four genetic letters (A [adenine], G [guanine], C [cytosine], and T [thymine]), instead of the binary values (1 and zero) used by standard computer systems. That is possible since small DNA molecules of each random string might be combined to order. An machine's input is thus displayed (within the utmost effective case) through DNA molecules with particular strings, the commands are performed by laboratory procedures at the molecules (together with selecting them related to size or reducing strands consisting a positive sub-string), and the output is identified as few assets of the very last group of molecules.

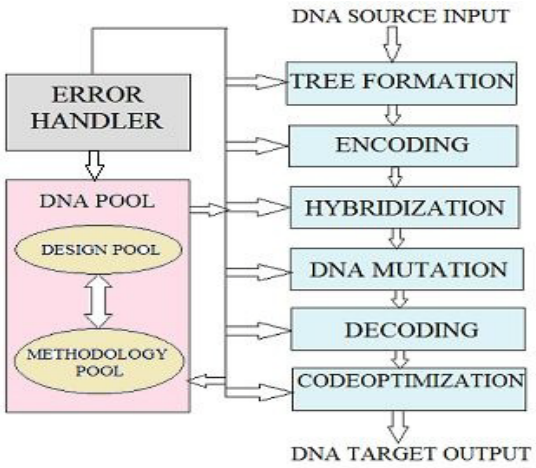

Figure 1 DNA computing method

1.2 DNA Cryptography

DNA cryptography includes enciphering the plaintext by use of DNA computational techniques. Most of the cryptographic procedures include a huge memory and

computations like, One Time Pad wherein there are non-repeating very huge textual content pads; this method might be very beneficial. A gram of DNA includes 1021 DNA bases and might store 108 terabytes of storage [4]. 1000000000000 bits of binary information may be saved in a single cubic decimeter of DNA solution [3]. Furthermore DNA based computations have very less time intake in comparison of different algorithms. The assignment of any cryptography set of rules is to comfy the records for extremely long period of time. In this approach, bases of DNA are organized in irregular order and plaintext bits may be saved efficiently by the use of those bases. As this method applies one time pad that is completely arbitrary cryptographic method, the information may be secured for extremely long durations of time. Similarly to storage space, DNA molecules posses parallel computation, which means DNA based approaches are capable of extreme processing. DNA chains have massive scale of parallelism and its computing pace could attain up to at least one billion instances in keeping with second computations [5]. DNA based computer systems additionally have very low power intake, that's equal to one – billionth of a conventional systems [5].

2. RELATED WORK

Raju, Parwekar et al. [5] represented two server password authenticated key exchange between two servers that is used to validate individual and so that hacking the passwords for hackers become very tough process. Additionally they proposed the DNA for Encryption and Decryption at the side of ElGamal Encryption approach. Vijayakumar, Zayaraz et al. [6] proposed DNA based Password authentication using Hyper Elliptic Curve Cryptography (HECC) technique. These machine posses the benefits of Hyperelliptic Curve Cryptography (HECC) approach that it has smaller key length, much less transmission and processing overhead for Password creation and signature confirmation procedure. Misbahuddin et al. [7] proposed a novel two-way secure authentication scheme using integration of DNA cryptography and Steganography for each security and usability. The protocol makes use of text and image password of which textual content password is transformed into cipher textual content using DNA cryptography and embedded into image password via making use of Steganography. Novak, Lukas et al. [8] proposed DNA based authentication of plant extracts which is beneficial and could reliably supplement chemical research. Moraes, nevertheless et al. [9] offered case histories where dietary supplements, decoctions, and different merchandise were proven to comprise materials aside from the main element specified at the label. They find that there is a crucial want for higher quality control in this organisation, which if now not unsolicited, which could arises from regulation. Soram, Khomdram et al. [10] proposed a technique to make use of biometric DNA records and the insubordination of Elliptic Curve Discrete Logarithm problem (ECDLP) for private authentication in data protection structures. They also give background knowledge on DNA and the elliptic curve discrete logarithm hassle, along with the generally implemented specific arithmetic. Hussain, Rahmana et al. [11] proposed a singular, secure, particular and effective DNA based encryption and decryption procedure and additionally offer an study of its overall performance. Gogte, Nemade et al. [12] proposed a imitation of quantum key alternate and authentication observed through an accomplishment of DNA based procedure for safe content sending and receiving.

3. COMPARISION TABLE

Table 1 Comparison of various DNA based authentication techniques

Year of publication	Name of the author	Title of the paper	Technique	Benefits	Limitations
2015	Raju P.V.S.N[5]	DNA Encryption Based Dual Server Password Authentication	DNA for Encryption and Decryption along with ElGamal Encryption scheme	This technique make very difficult to hack passwords for hackers.	High power consumption.
2014	Vijayakumar[6]	DNA based Password Authentication Scheme using Hyperelliptic Curve Cryptography for Smart Card	Hyper Elliptic Curve Cryptography (HECC) scheme	This technique has many advantages like small key size, less communication and computational overhead and less power consumption etc	Large data storage capacity is needed.
2015	Mohammed Misbahuddin[7]	A Secure Image-Based Authentication Scheme Employing DNA	A novel two-way secure authentication scheme using DNA cryptography	It makes the system more secure and increase usability.	The research of DNA cryptosystem lacks practical implementation

		Crypto and Steganography	and Steganography		
2007	Johannes Novak[8]	DNA-based authentication of plant extracts	An Isolated DNA authentication method	This technique is very feasible and reliable.	It provides unambiguous plant identification and also provide quality, safety and efficacy of a drug
2015	Denise F. Coutinho[9]	DNA-Based Authentication of Botanicals and Plant-Derived Dietary Supplements	DNA based bar coding method	This paper gives information that how we can provide greater authority and resolution for identifying the products.	There is still great need for quality control in plant derived dietary supplements.
2010	Ranbir Soram[10]	Biometric DNA and ECDLP-based Personal Authentication System: A Superior Posse of Security	Elliptic Curve Discrete Logarithm Problem (ECDLP)	The paper shows that DNA is most distinct , highly accurate and very stable method for personal authentication systems	The cost of DNA analysis is very high and it is not a real-time method.
2014	Noorul Hussain[11]	A Novel DNA Computing based Encryption and Decryption Algorithm	A novel, secure and dynamic DNA based encryption and decryption algorithm along with Central Dogma of Molecular Biology (CDMB) concept.	This technique presents the robust encoding and dynamicity of encryption process.	NA
2013	Sharvari godte[12]	Simulation of quantum cryptography and use of DNA based algorithm for secure communication	BB84 protocol	This method prevents the communication from eavesdropping, middle attack, spoofing, packet sniffing and replay attack	It does not provide Protection against denial of service attack and is not suitable for long distances communication.

4. CONCLUSION

Deoxyribonucleic acid method is evolved in lots of programs which include password authentication, image encryption, Botanicals and Plant-Derived nutritional dietary supplements etc. This paper discussed diverse DNA based authentication strategies for data protection. We additionally mention numerous advantages and obstacles in relation to DNA authentication methods. Presently DNA strategies maintain suitable security with smaller key length as compare to all other authentication strategies. After discussing various DNA based techniques we comprehend that it has many advantages over the conventional techniques which include low power consumption, lesser computational overhead, lesser time intake and huge storage potential and so forth. Beside so many achievable advantages over conventional techniques, DNA computing has high-quality capacity for practical use.

REFERENCES

[1] Amosa M, Paun G, Rozenbergd G. " Topics in the theory of DNA computing[J]". Theoretical Computer Science 287 (2002) 3-38.

[2] Guozhen Xiao." New field of cryptography: DNA cryptography[J]" Chinest Science Bulletin 2006 51(10): 1139-1144.

[3] Gehani A, LaBean T. "DNA-based cryptography". Dismacs Series in Discrete Mathematics and Theoretical Computer Science 2000 54: 233-249.

[4] Radu Terec . "DNA Security using Symmetric and Asymmetric Cryptography", IJNCAA (ISSN 2220-9085), 2011 Yunpeng Zhang and Liu He Bochen Fu. "Research on DNA Cryptography, Applied Cryptography and Network Security", Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0218-2, InTech, 2012.

[5] Raju P.V.S.N, Parwekar P. "DNA Encryption Based Dual Server Password Authentication" Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014

[6] Vijayakumar, Vijayalakshmi, Zayaraz. "DNA based Password Authentication Scheme using Hyperelliptic Curve Cryptography for Smart Card" Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC

[7] Mohammed Misbahuddin. **"**A Secure Image-Based Authentication Scheme Employing DNA Crypto and Steganography" Proceedings of the Third International Symposium on Women in Computing and Informatics

[8] Johannes Novak, Sabine Grausgruber-Gröger, Brigitte Lukas. "DNA-based authentication of plant extracts"Food Research International 40(3):388-392 · April 2007

[9] Denise F. Coutinho Moraes, David W. Still, Michelle R. Lum, Ann M. Hirsch. "DNA-Based Authentication of Botanicals and Plant-Derived Dietary Supplements" Planta Med © Georg Thieme Verlag KG Stuttgart · New York · ISSN 0032-0943

[10] Ranbir Soram, Memeta Khomdram. "Biometric DNA and ECDLP-based Personal Authentication System: A Superior Posse of Security" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010

[11] Noorul Hussain, Ubaidur Rahmana, Chithralekha Balamuruganb, Rajapandian Mariappanc. "A Novel DNA Computing based Encryption and Decryption Algorithm" International Conference on Information and Communication Technologies (ICICT 2014)

[12] Sharvari gogte, Trupti nemade, Shweta pawar, Prajakta nalawade. "Simulation of quantum cryptography and use of DNA based algorithm for secure communication" IOSR journal of computer engineering (IOSR-JCE), volume 11, issue 2(may-june 2013)