Secure communication technique using Lorenz cipher and SHA Algorithm

[1]Vishnu Dadu Panthi,[2]Gajendra Shrimal
[1]M.Tech Research Scholar , [2]Asst. Professor ,
[1,2] Department of Computer Science and Engineering
Jagannath University, Jaipur , Rajasthan, India.

Abstract : Data security is a huge issue for affiliations and affiliations today. Guaranteeing that your data is secure is winding up progressively essential dependably and fundamental to business assignments. Encryption is the technique through which data is shielded from deplorable eyes. Encryption is the best sort of data security; at any rate disastrously, it is correspondingly a zone that not many individuals acknowledge how to approach. The proposition concentrated on influencing the utilization of the Lorenz To figure with SHA 256 for secures the data send to the target machine , utilizing the SHA 256..

With the Lorenz Cipher not simply extended the entropy of the figure message yet also leads in endorsing the authenticity of data as the changed over plaintext SHA-256 code is composed with the SHA-256 code gave from the sender end.

Index Terms – **Encryption , Decryption , Lorenz Cipher, SHA 256**

I. INTRODUCTION

Web Identity (IID), in like way on-line character or web persona could be a social character that a web client sets up in online frameworks and regions. It will in like way be considered as An effectively planned introduction of oneself. In any case, a couple of individuals utilize their veritable names on the on the web, some net purchasers wish to be dark, trademark themselves by ways for pen names, reliably changing extents of in the long run acknowledgeable information. a web character may even be constrained by a client's relationship to a particular exhibit they're a piece of on the on the web. Some will even be outrageous regarding their character.

In some on-line settings, similarly as net talks, on-line visits, and inconceivably multiplayer on-line dissimulation amusements (MMORPGs), purchasers will address themselves remotely by picking a logo, a logo evaluated sensible picture. Pictures square measure a system purchasers unmitigated their on-line character. Through participation with astonishing purchasers, a getting together on-line character gets a lowness, that empowers altogether unforeseen purchasers to choose whether the aura is worth of trust. on-line characters square measure related with purchasers through endorsement, that typically needs voyage through commitment and correspondence by means of signals in. a couple of goals in like way utilize the client's data dealing with pass on or following treats to perceive purchasers.

There square measure fundamentally 2 explanations behind limiting a client to a character:

- The client demeanor could be a parameter in get the chance to oversee conclusions
- The client demeanor is recorded once work security-huge occasions in an exceedingly overview way.

The essential job is required for the structure to connect with coarseness in find the opportunity to control. inside the event that we don't grasp World Health Organization the client is we won't appreciate the client's privileges, aside from single client structures. crafted by an attitude isn't significant for physical purchasers, structure outlines what's more need find the opportunity to control and will be seen. The subsequent explanation empowers the structure to relate logged occasions to characters. Since this speculation is generally vexed with respect to security,security occasions square measure most principal, anyway work framework occasions contains analtogether additional start to finish use than straightforward security. work framework occasions will support in finding strategy and utilitarian confounds and is fundamental with structure fixes.

Another field during which work expect a focal half is inside the progression of client charge. The utilization of a readied mien conversing with the physical client is, as plot higher than, fundamental for security structures like affirmation. At the explanation once the framework has attested the character, get the chance to oversee handles the great conditions related therewith personality [1]

1.1 Lorenz Cipher

English cryptanalysts, one who proposed blended German teleprinter advancement as the Fish, named the machines and besides its development Tunny which means the tunafish and decided its clear structure in the three years as of now what they saw the machines. The SZ machines are one were the in-line relationship with direct teleprinters. Additionally, the undertaking partners utilizing SZ40 based machines that was begun in the hour of June 1941. Moreover the improved SZ42 based machines that were in like manner brought into liberal use the from in the hour of mid-1942 ahead for unordinary state correspondences between the German boss in the Wünsdorf on which is close to the Berlin, and military Commands during had Europe.[1] Also the more framed SZ42A came into the typical use in Feb 1943 and besides SZ42B in the hour of June 1944.[1]

Remote media transmission (WT) as fundamental show up line circuits are similarly used with the ultimate objective of this traffic.[4] And also these of the non-Morse (NoMo) messages are moreover were gotten the Britain's Y-stations organized at Knockholt and Scandinavian country Hill and besides sent to the Government Based Code and Cipher school at the Bletchley Park (BP). Furthermore some were then deciphered by utilizing hand frameworks before the strategy was in like manner for the most part robotized, first with the Robinson machines and in this way with the Colossus computers.[4] The deciphered Konrad Zacharias Lorenz messages made a boss among the essential imperative duties to British outrageous military comprehension and to Allied triumph in Europe, because of the irregular state huge natures of the information that was gotten from Konrad Zacharias Lorenz based decrypts.[1]

XOR truth table

A	BA⊕ B	
0	0	0
0	1	1
1	0	1
1	1	0

Other of the names for this limit are: Not approach (NEQ), the modulo 2 development that are without 'pass on' and besides the modulo 2 subtraction one that are without 'get'. Vernam's cipher is the Symmetric-key figuring, that is. a comparable key is in like manner used both to encipher the plaintext in order to make the cipher-content and to decipher the cipher-message in order to yields the first or the real plaintext:

Plaint-ext⊕ key = cipher-content

moreover,

cipher-text⊕ key = plain-content. [2]

II. Related Work

Alshammari, et. Al 2017, another cryptosystem approach in light-weight of Lorenz insane structures is shown for secure data transmission. What's more, moreover the framework utilizes a stream figure, during which the encoding key changes indefatigably. Other than at any rate one among the parameters of the Konrad Zacharias Lorenz generator is constrained by accomplice degree right hand rough generator for swollen security. The framework is dead by utilizing 2 separate Spartan six FPGA sheets. Security assessment (Section VII) shows the framework to have a strange condition of security showed up contrastingly in connection to elective correspondence structures. This paper shows a refined correspondence structure with high security in light-weight of Konrad Zacharias Lorenz stream figure. The structure is genuine utilizing 2 separate Spartan six FPGA sheets. the data encoding depends upon 2 Lorenz Generators (Main and Auxiliary).

Kothari et. Al 2017, Today's presence is moved period, everybody filters for data on Web. The web isn't space for data, yet in particular, it is a contraption to relate individuals. Individuals used to share data and exchange described data on the Web. Since Internet is wholeheartedly open verifying data on Web is a lot of principal, two or three structures are depended upon to cover this data. There are different strategies available to camouflage the data, for instance Steganography, cryptography and so forth. The upside of steganography over cryptography is that nobody close to the sender and recipient can see the message. This paper revolves around various steganography strategies to cover the data on Web.

Hamdaneet. Al 2017, Named Data Networking (NDN) addresses a rising Information-Centric Networking planning. It sees data as the focal part and it impacts in-arrange sparing. With the last part, standard security portions, associated with data zone, can never again be utilized. That is the explanation a data driven security show is gotten a handle on. This model depends fundamentally on the advancement of an engraving to the majority of the recouped data. Notwithstanding, the engraving check requires the fitting open key. To trust in this key, NDN gives an enrapturing stage, supporting various models.

Li et. Al 2016, In this paper, a high-adaptability and importance fruitful reconfigurable standard cryptological processor style is exhibited, that depends upon long course word (VLIW) structure. By isolating fundamental endeavors and limit qualities of balanced figures, the application-explicit heading set structure for standard figures is organized. Eleven kinds of reconfigurable cryptological science units are expected to help indisputable task modes and parameters for standard figures. it's been made with zero.18μm CMOS headway, the research results display that the most outrageous excess can do 200MHz.

Dhillon and Kalra2016 , Internet of things (IoT) is a making game plan of presented gadgets that can talk with the outside condition. With this broadening in general system, electronic correspondence between gadgets is persuading the chance to be remote and unavoidable. Moreover, a tremendous portion of the IoT associations will be perceived as ceaseless presented frameworks which depend overwhelmingly on security instruments. This makes security crucial to installed contraptions in IoT.

III. PROPOSED WORK

3.1 Algorithm for Encryption

The algorithm for the encryption of the plain text to cipher text is explained below:-

Step 1 : Read PTEXT,EKEY.

Step 2: Set N = LENGTH (PTEXT).

Step 3: Set M = LENGTH (EKEY).

Step 4: If N>M then :

Repeat String pattern of EKEY to become same size of PTEXT.

[End of If structure]

Step 5: Set BTEXT=CONVERT2BINARY (PTEXT).

Step 6: Set BEKEY=CONVERT2BINARY (PTEXT).

Step 7: Set XDATA=XORVALUE (BPTEXT,BEKEY).

Step 8: Set SHATEXT=HASH (PTEXT).

Step 8: Set ETEXT=Binary2String (XDATA)+SHAPTEXT.

Step 9 : Write ETEXT.

Step 10: Stop.

3.2 Algorithm for Decryption

The algorithm for the decryption of the cipher text to plain text is explained below:-

Step 1: Read ETEXT, EKEY, N (Number of Characters in EKEY).

Step 2: Extract First N Characters of ETEXT to ETEXT2 and remaining characters to ETEXT3.

Step 3: Set BTEXT=CONVERT2BINARY (ETEXT3).

Step 4: Set BKEY=CONVERT2BINARY (EKEY).

Step 5 : Set XDATA=XORVALUE(BTEXT,BKEY).

Step 6: Set DTEXT=BINARY2STRING (XDATA).

Step 7: Set SHADTEXT=HASH(DTEXT).

Step 8: If SHADTEXT=ETEXT3 then:

Write "Successful Decryption".

Else :

Write "Not a Successful Decryption".

[End of If Structure]

Step 9: Stop.

IV. IMPLEMENTATION AND RESULT ANALYSIS

The implementation of the proposed work is done using the Micosoft Visual Studio 2010 and the SQL Server Express 2008 edition is used for the database purpose.

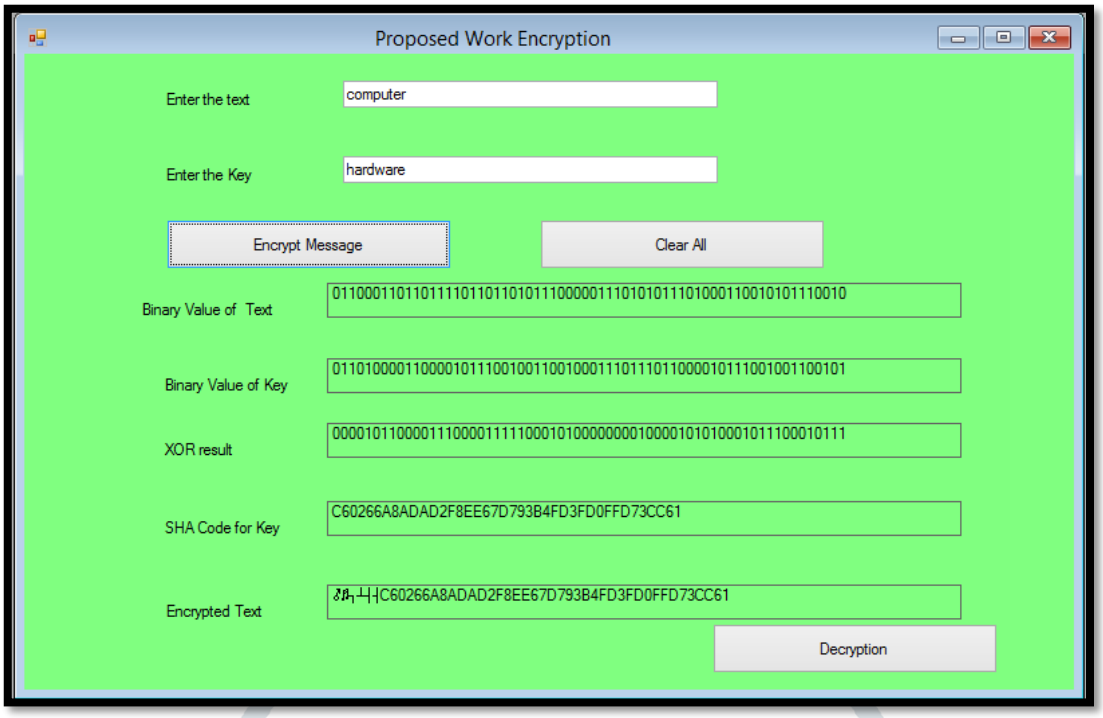

Fig 1. Proposed Work Encryption

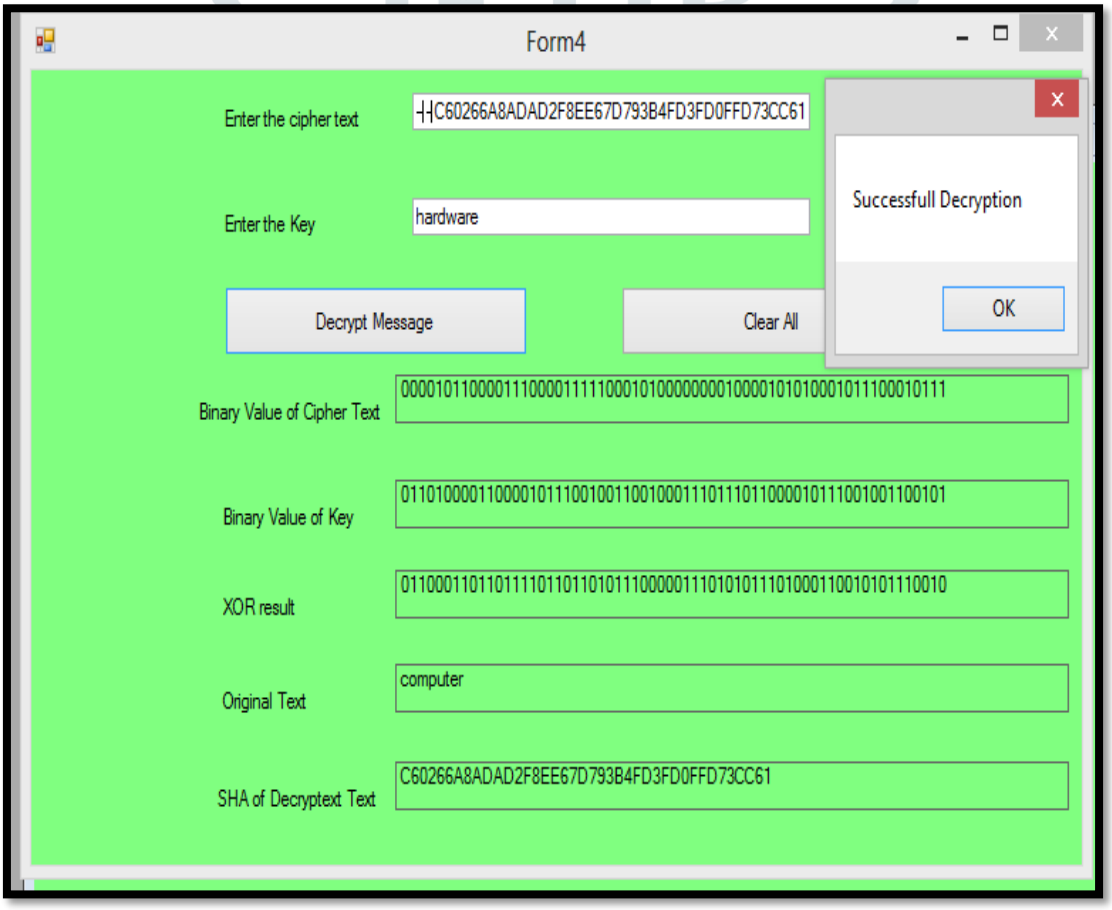

Fig 2. Proposed Work Decryption

TABLE 1 TEST RESULT ANALYSIS TABLE FOR BASE KEY

Base Key	Website/Tool	Result
♪♬¶ㄱ丄ㅓㅓ	Password Meter	Score : 82 Strong
♪♬¶ㄱ丄ㅓㅓ	Password Checker	Strength : 33% low
♪♬¶ㄱ丄ㅓㅓ	Cryptool2	Entropy 2.674 Strong

TABLE 2 TEST RESULT ANALYSIS TABLE FOR PROPOSED KEY

Proposed Key	Website/Tool	Result
♪♬¶ㄱ丄ㅓㅓaa97302150fce811425cd84537028a5afbe37e3f1362ad45a51d467e17afdc9c	Password Meter	Score : 100% Very Strong
♪♬¶ㄱ丄ㅓㅓaa97302150fce811425cd84537028a5afbe37e3f1362ad45a51d467e17afdc9c	Password Checker	Strength : 100% Excellent
♪♬¶ㄱ丄ㅓㅓaa97302150fce811425cd84537028a5afbe37e3f1362ad45a51d467e17afdc9c	Cryptool2	Entropy 4.372 Very Strong

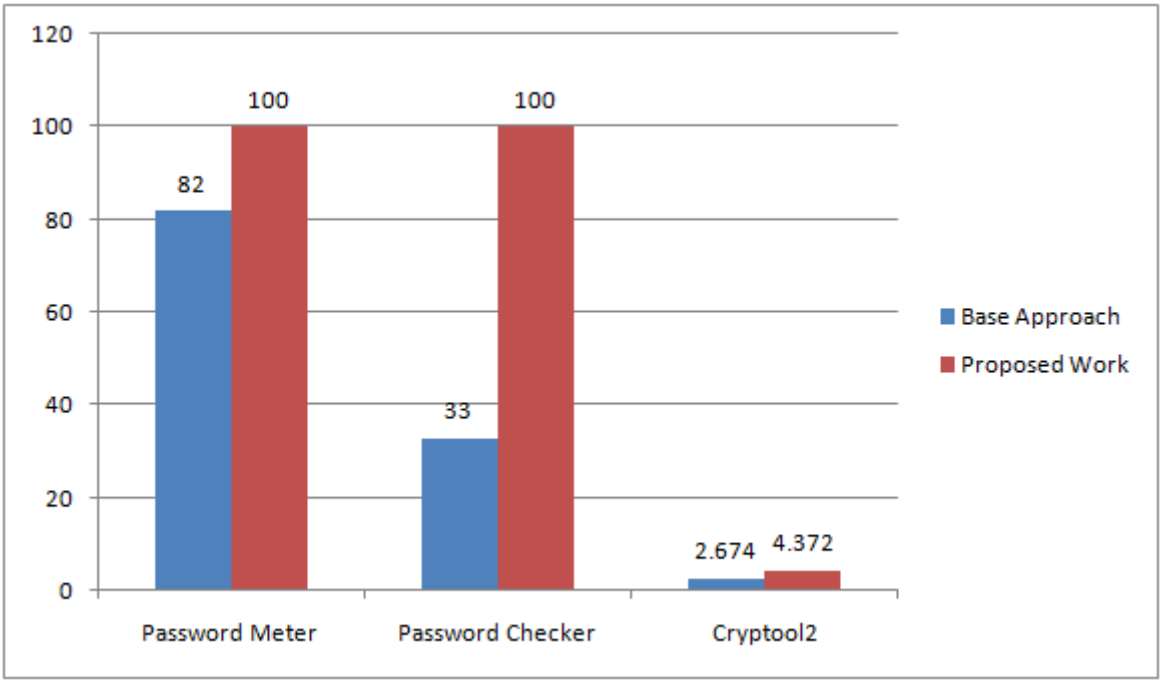

Fig 3. Graphical Comparison of Base and Proposed Approach

V. CONCLUSION

System security is that the any affirmation of access, abuse, and hacking of reports and inventories in a very PC arranged structure. while not an uncertainty the principal rudimentary hazards to a system intertwine sicknesses, worms, spyware, adware and information misrepresentation. A victor among the preeminent basic things of structure security is that the changed layers of security. there's no single pack or structure that may give fruition affirmation against each peril to your system, hence it's rudimentary to make some degree to utilize totally various layers of security for your system.

The anticipated system exploitation the possibility of the Konrad Lorenz Cipher and SHA-256algorithm improved the wellbeing and can have broadened the weight on the code specialists to a large portion of the cipher content , resultant in partner degree

unrealistically secure cipher content. In the anticipated work, the resultant cipher substance is attempted over the different on the on the web and isolates instruments for testing the character of the cipher and in this manner the outcome got ar very remarkable..

REFERENCES

1. Dr. SandeepTayal, Dr.Nipin Gupta, Dr. Pankaj Gupta, "A Review paper on Network Security and Cryptography",Advances in Computational Sciences and Technology ,2017
2. Neha Sharma, Prabhjot, Er. Harpreetkaur "A Review of Information Security using Cryptography Technique ",International Journal of Advanced Research in Computer Science ,2017
3. A.S. Alshammari, M. I. Sobhy and P. Lee, "Secure digital communication based on Lorenz stream cipher," 2017 30th IEEE International System-on-Chip Conference (SOCC), Munich, 2017, pp. 23-28.
4. Lipi Kothari, RikinThakkar, SatvikKhara,"Data hiding on web using combination of Steganography and Cryptography" , IEEE2017
5. A.Hamdane, R. Boussada, M. E. Elhdhili and S. G. E. Fatmi, "Hierarchical Identity Based Cryptography for Security and Trust in Named Data Networking," 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Poznan, 2017, pp. 226-231.
6. Wei Li, XiaoyangZeng, Longmei Nan, Tao Chen and Zibin Dai, "A high-flexibility and energy-efficient application-specific cryptography VLIW processor for symmetric cipher algorithms," 2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Hangzhou, 2016, pp. 1281-1284.
7. P. K. Dhillon and S. Kalra, "Elliptic curve cryptography for real time embedded systems in IoT networks," 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON), Rajpura, 2016, pp. 1-6.
8. A. Mirtalebi and S. M. Babamir, "A cryptography approach on security layer of web service," 2016 IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), Baku, 2016, pp. 1-5.
9. K. P. Singh, V. Kumar, S. Singhai and D. Sehjal, "Design and implementation of cryptography based attitude and heading reference system with Extended Kalman Filter," 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON), Rajpura, 2016, pp. 1-6.
10. A. Sanada, Y. Nogami, K. Iokibe and M. A. Khandaker, "Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography," 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), Taipei, 2017, pp. 287-288.
11. S. Z. Arnosti, R. M. Pires and K. R. L. J. C. Branco, "Evaluation of cryptography applied to broadcast storm mitigation algorithms in FANETs," 2017 International Conference on Unmanned Aircraft Systems (ICUAS), Miami, FL, USA, 2017, pp. 1368-1377.
12. H. Thapliyal, T. S. S. Varun and S. D. Kumar, "Adiabatic Computing Based Low-Power and DPA-Resistant Lightweight Cryptography for IoT Devices," 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, 2017, pp. 621-626.
13. Z. Pan and L. Zhang, "Optical Cryptography-Based Temporal Ghost Imaging With Chaotic Laser," in IEEE Photonics Technology Letters, vol. 29, no. 16, pp. 1289-1292, 15 Aug.15, 2017.
14. R. Bassous, H. Fu and Y. Zhu, "Ambiguous Multi-symmetric Cryptography Proof of Concept and Experiments," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 231-236.
15. A.Sarkar and B. K. Singh, "Cancelable biometric based key generation for symmetric cryptography," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2017, pp. 404-409.
16. Jongho Won, AnkushSingla, Elisa Bertino,"CertificateLess Cryptography-Based Rule Management Protocol for Advanced Mission Delivery Networks",IEEE,2017
17. J. H. Jeong, J. O. Kim, T. Y. Kim and J. R. Choi, "Reconfigurable array-based design for flexible cryptography chip architecture," 2017 13th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME), Giardini Naxos, 2017, pp. 345-348.
18. S. Lee and K. Shin, "An efficient implementation of SHA processor including three hash algorithms (SHA-512, SHA-512/224, SHA-512/256)," 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, 2018, pp. 1-4.
19. S. S. Omran and L. F. Jumma, "Design of SHA-1 & SHA-2 MIPS processor using FPGA," 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, 2017, pp. 268-273.
20. K. A. Nugroho, A. Hangga and I. M. Sudana, "SHA-2 and SHA-3 based sequence randomization algorithm," 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, 2016, pp. 150-154.