International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52310561

A Literature Survey on Securing Internet of Things (IoT) Devices : AES vs Simon-Speck Encryptions

[1]Sonam Rajput, [2]Dr. Arvind Kaurav, [3]Prof. Nehul Mathur
[1]M.Tech Scholar, [2]Professor, [3]Assistant Professor
[1,2,3] Department of Electronics and Communication (EC), Bhopal Institute of Technology, Bhopal, Madhya Pradesh, India

ARTICLEINFO

Article History:

Accepted: 30 Sep 2023
Published: 27 Oct 2023

Publication Issue
Volume 10, Issue 5
September-October-2023
Page Number
588-595

ABSTRACT

Internet based secure data transmission is an emerging area of research, where most of the data transfer infrastructure is moving to make their service and delivery more efficient. In this paper our work approach lead behind the secure data transmission data get upload over the data server and its different user due to different ownership. AES is a well-established encryption standard that has been extensively analysed and widely adopted in various industries and applications. It is considered highly secure and has withstood rigorous cryptographic scrutiny. In this survey discuss In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Only authorized parties can decipher a cipher text back to plaintext and access the original information. Also the process of decryption of an AES cipher text is similar to the encryption process in the reverse order.

Keywords : Asymmetric Encryption System (AES), Simple Hash Algorithms (SHA),National Security Agency (NSA), Secure Data Transmission, MD-5, block size, word size, hash output , number of round and Finite Field Construction.

I. INTRODUCTION

Encryption is based on cryptography. Cryptography is the art of hiding information to make it unreadable without special knowledge or a key. The earliest recorded examples include the use of non-standard hieroglyphs as a substitute for the hidden information, and the use of personal identification marks such as seals, emblems, or logos for authentication. The receiver of the sealed item would have a copy of the true mark to use to authenticate the one presented (these are the precursors of signature verification).

Encryption allows a person to hide the meaning of information or messages in such a way that only those who know the secret method may read them. For a very long time, people have had many different

reasons for wanting to hide information from others. The earliest historic examples were for hiding trade secrets, military secrets, and secret correspondences between spies and lovers. These same encryption principles are now used to safeguard your internet communications.

II. DENCRYPTION

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as cipher text. Only authorized parties can decipher a cipher text back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. Historically, various forms of encryption have been used to aid in cryptography

A. Encryption In Cryptography

In the context of cryptography, encryption serves as a mechanism to ensure confidentiality. Since data may be visible on the Internet, sensitive information such as passwords and personal communication may be exposed to potential interceptors. To protect this information, encryption algorithms convert plaintext into cipher text to transform the original data to a non-readable format accessible only to authorized parties who can decrypt the data back to a readable format.

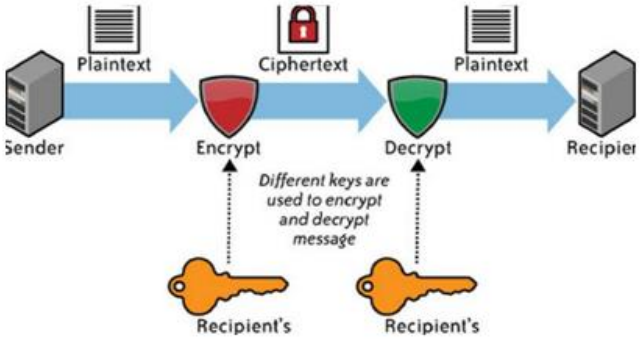

Fig 1 Context of Cryptography Encryption Serves

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in every spherical are in reverse manner, not like for a Feistel Cipher, the encryption and decryption algorithms desires to be one at a time implemented, though they are very carefully related.

B. Terminologies Of Cryptography

The often used phrases in cryptography are defined right here-

Plain Text - The undeniable textual content message is the textual content which is readable and can be understood by using all users. The simple textual content is the message which undergoes cryptography.

Cipher Text - Cipher textual content is the message got after making use of cryptography on simple text.

Encryption - The procedure of changing undeniable textual content to cipher textual content is referred to as encryption. It is additionally referred to as as encoding.

Decryption - The manner of changing cipher textual content to simple textual content is referred to as decryption. It is additionally termed as decoding.

III.LITERATURE SURVEY

Ananya B L, et.al. (22 March 2023) - Nowadays data sharing over the internet is a major and critical issue due to security problems. So more security mechanisms are required to protect the data while sharing through an unsecured channel. we present one such algorithm for data confidentiality while sharing. Advanced Encryption Algorithm (AES) is a symmetric encryption algorithm that provides more encryption security than its predecessor Data Encryption Standard (DES). In this review paper, we compare the various applications, advantages, and shortcomings of this complex algorithm by also comparing them to other standard algorithms [01].

Rahul Neve et.al. (16 July 2023) - The lightweight cryptographic (LWC) algorithm is used for resource constraint devices. The performance analysis and development of LWC is for achieving better data security in resource constrained mobile devices for effective implementation. Literature survey on LWC was carried out where it was observed that the implementation of two well-known algorithms "SIMON" and "SPECK" are in latest research as per future technological requirements. On comparing SIMON & SPECK algorithms with conventional blocks, lightweight block ciphers the following challenges that are required to be mitigated by including usage of minimal hardware overhead in proposed design (e.g., time, memory consumption), viz. use of low-cost smart mobile devices, with minimal power, low energy consumption and improved security performance. Algorithms were implemented on the Raspberry Pi 3 with 1GB RAM, Quad Core 1.2GHz Broadcom BCM2837, with 32-bit Raspbian Operating System of 5V and current of 2 mA. Input to the algorithm is fed as text with varying size viz. 100kB, 200kB, 300kB, 400kB, 500kB.An attempt is made to developed hybrid LWC algorithm by using key scheduling logic of SPECK and Round function logic of SIMON [02].

Baiq Yuniar Yustiarini et.al. (07 September 2022) - Delivering information from Internet of Things (IoT) devices to a cloud server possesses several security issues, e.g. information eavesdropping, modification, and theft. Therefore, communication between IoT devices and the cloud server should be protected by encryption methods. However, there are few encryption techniques options that are suitable for the need for lightweight communication as demanded by the IoT devices. Due to these circumstances, the NSA launched an encryption algorithm for IoT named Simon and Speck, which are maximally efficient while still providing the advertised level of security, as determined by the key size. This study aims to test and compare the Simon-Speck and AES encryption algorithms and their effect on networking performance on IoT devices. The parameters in this test are delay, throughput, the efficiency of memory usage from the encryption algorithm, and the value of the avalanche effect. Experimental results show that the Speck algorithm outperforms the Simon and the AES algorithms in terms of communication delay and memory usage. Regarding the avalanche effect values, the Simon algorithm possesses the highest avalanche effect value on average against the Speck and the AES algorithms [03].

L.Mary Shamala et.al. (2021) - Internet of Things is a worldwide set-up of interconnected entities that permits millions of devices to communicate with each other. Combined with reliable communication, ensuring security concerning confidentiality, integrity, and authenticity is a great challenge in IoT. Unsecured IoT devices open gateway for attacks. Unprotected and vulnerable devices, at times, allow easy entry for hackers, enabling them to have access to the shared network and personal, corporate assets. Conventional security measures are not suitable and cannot be applied to IoT technologies because of their minimum storage, low processing capacity, and limited computing power. Besides, scalability and heterogeneity issues arise when a variety of devices are interconnected. This paper presents the security

threats and requirements of IoT cryptography, technology, and trends. The paper also discusses the challenges faced and the comparison of solutions already existing in IoT security [04].

Pejman Panahi et.al. (13 January 2021) - All smartphones, notebooks, or other communication devices could connect to the cloud, so the data are accessible everywhere. When these devices are interconnected through the internet, they make an Internet of Things (IoT) network that exchanges data among network nodes and other services. IoT has a broad application area from smart applications to various industrial usages. However, the high volume of data transferred in the IoT network makes it crucial to implement mechanisms to transfer the data safe and secure. Enciphering is one of the best techniques to ofer end-to-end security [05].

Abdulrazzaq H. A. Al-Ahdal et.al. (31 Oct 2020) - Modern applications consist of different types of control devices and sensors that connect to the Internet. These applications are new approved technologies called the Internet of Things. Nowadays, these new technologies have gained a great interest in the field of research because of their existence in several diverse fields and due to the rapid development of these technologies. Communication between these devices generates a large amount of private and sensitive information and data between them. Therefore, maintaining the confidentiality of that data and information in the Internet of Things is of great importance. Mathematical cost (complex mathematical operations) and the number of cycles in traditional cryptographic algorithms leads to a large use of memory and energy waste for devices with limited resources, which makes traditional cipher algorithms inappropriate for Internet of Things devices. A fast and LW algorithm called NLBSIT has been proposed in this regard, which provides the requisite protection and resource constrained confidentiality of data on IoT devices. This algorithm (NLBSIT) uses a 64-bit key to encode 64-bit data, uses simple mathematical operations (XOR, XNOR, shifting, swapping), and uses the features of both the Feistel and SP Network architecture to achieve diffusion and confusion (increasing data security). The FELICS and MATLAB tools are used to simulate the NLBSIT algorithm. To execute this algorithm, various data types are used, such as text and images. The results of the simulation indicate the supremacy of the proposed algorithm in various areas, such as security efficiency, less cycles (encryption and decryption), and less memory usage [06].

Li Ning et.al. (2020) - The most serious challenges currently faced by healthcare environment is the decision making related to the installation of the most suitable and appropriate lightweight authentication cipher that could provide solutions towards the authentication issues prevailing in IoHT devices. This decision making becomes more troublesome and tricky due to the number of factors that are taken into account such as availability of many existing ciphers, complex and multiple numbers of requirements involved and frequent changing of these requirements from one platform to another. This decision making is also hampered by the nature of IoT devices operating in healthcare environment as they come up with limited functionality, processing, bandwidth and memory. In this regard, we present an evaluation framework focuses upon the selection of best light weight cryptographic ciphers by considering the most important parameters or requirements of criteria. The proposed framework considers the requirements like performance, physical and security as suggested by widely accepted standards such as National Institute of Standards and Technology (NIST) and International Standard Organization standard such as ISO/IEC 29192 for building evaluation criteria. This framework evaluates and selects the best lightweight cryptographic among the 10 ciphers i.e. PRESENT-80, Scalable Encryption Algorithm (SEA), HIGHT, Lightweight Encryption Algorithm (LEA) Advanced Encryption Standard (AES-128), mCrypton, NOEKEON, Klein, Camellia and Tiny Encryption

Algorithm (TEA) for the purpose of evaluation in IoHT environment [07].

Chandel, et.al. (2019, December) -The present study Nowadays, using of internet is increasing. Everyone is more active on the social networking sites and data exchange has been increased rapidly. Here, data security plays a vital role. Encryption and decryption algorithms are used to escape the data from any third party attacks. There are use various type of cryptographic algorithms to encrypt data. AES algorithm is more widely used as a symmetric encryption algorithm and it is easy to use and robust. AES is the most powerful cryptographic algorithm which is used in most of the applications which we use in our daily lives like messenger etc. AES cryptography packages are available almost on every platform such as Turbo C++, DEV C+ + etc. There are encrypt and decrypt the data using different combinations from the malicious attack. This algorithm give different key sizes for encryption 10, 11 and 14 rounds which are used for 128-bit, 192-bit key and 256-bits block cipher respectively. In RSA it is an asymmetric type of cryptography i.e. there are 2 keys used open key and private key and we are using the product of any 2 large prime number for the purpose of security. RSA is more thread safe [08].

Hafsa, et.al. (2019, March) - This paper reviews suggested a novel hybrid cryptosystem that uses advantages of both symmetric key and asymmetric cryptographic ways. The main of the proposed architecture is a modular multiplication unit, which extends operations realized for an optimized ECC cryptosystem in order to support the Mix Columns operation of an optimized AES algorithm. There are evaluated our system design on DE2-115 board. Findings proved that our proposed method demands less execution time, less area occupation and less total power dissipation compared with others methods. As a continuity to this work, we propose to design an optimized Elliptic Curve Digital Signature (ECDSA) cryptosystem which can be implemented in one ARM based on MP core SoC such as with Zynq FPGA. This prototype will be applied in several input conditions like images and video signals. To prove the security of the proposed system, hardware countermeasures against Side-Channel Attacks (SCA) will be studied and proposed [09].

Ghosh, et.al. (2019, December) - Several approaches of secured message transactions on cloud data are studied and analyzed. A secured cloud data message transaction protocol with variable length key has been designed, developed and applied through the use of Advanced Encryption Standard (AES) using the Python programming language. The length of the used key is given as input by the user followed by the selection of a secret key which is fed into the AES cryptographic system with the desired cloud data message thus producing the Cipher text that is to be transmitted to the destination. In the receiver end, the reverse process is performed with the same key on the received Cipher text and the plaintext is retrieved. A comparative study with the two existing approaches has been performed and presented. The presented security mechanism can be applied on any secured cloud data message transactions that may be either in financial or in e-commerce based cloud environment [10].

Sönmez, et.al. (2019, September) - Two important features have been selected for this attack. Which of these features is better can be understood by looking at the auc (area under curve) values in the Table II. Among the applied models, XGBoost and Random forest have the highest auc values. These models considered the" cycle on average" feature more important. Since the" deviation of cycle" feature was more important than the GBM and Decision Tree models, the auc value was slightly lower. When these results are compared, it is seen that the" cycle on average" feature is a more significant side channel leakage for time-driven cache attacks [11].

Bhattacharjya, et.al. (2019) - So at the beginning of discussing the major contributions of the work, lets

discuss the encryption level contribution, the SHRSA messaging scheme's 9 layered cipher's encryption with 1024 Bit RSA modulus, is shielding us from some of the scientic problems of RSA like, the very high computationally costly exponentiation modulo N problem, the exploitation of multiplicative property, low modular complexity with effortlessness, difficulty of the integer factorization problem of RSA, the exploitation of homomorphism property and speediness problem. There all know that all available RSA variants' encryption are able to solve two or three major problems of RSA but the SHRSA messaging scheme's encryption is resolving many problems of RSA as discussed in section III and section IV in details. Also the SHRSA messaging scheme's 9 layered cipher's encryption has proper protection from CCA and Short Plain- text Attack etc, along with protection to Snifng attack and the real-time Key negotiation issue also. Brute force attack is shielded by randomly changing the keys in synchronous time slot with 1024 Bit value [12].

Shvartsman, et.al. (2019, October) - A masking scheme for AES is presented which uses finite field construction variation with random masking to prevent higher-order power analysis. Field constructions are chosen to remove the co-variance between share leakage. Security analysis shows that this provides a high level of security against higher-order power analysis attacks. Although, the scheme requires inserting constant binary mapping matrices and a larger MixbColumns, the number of required registers is greatly reduced. As a result, 12% few logic gates are needed compared to the previous best design [13].

Iavich, et.al. (2018, October) - This paper reviews is described and analyzed two types of systems: Symmetric and Asymmetric cryptosystems. The paper provides new model of hybrid algorithm using AES and ElGamal cryptosystems. Special software tool was created and implemented for proposed system. Compared with encryption and decryption speed experimental research shows, that symmetric algorithm AES is faster, but asymmetric algorithm ElGamal is better to provide security. The symmetric algorithm AES requires very low computational power. AES is one of the best algorithms of symmetric encryption cryptography. ElGamal algorithm gives high throughput as compared to AES and other algorithms. The hybrid of AES and ElGamal algorithm has characteristics of both the algorithms. This makes the algorithm strong against vulnerabilities. This hybrid structure of AES and ElGamal provides more security by increasing the complexity. As the result shows, proposed AES & ElGamal hybrid algorithm model is comparatively better than ElGamal in terms of encryption / decryption time and better than AES in terms of its security. The complexity of the system is provided by combination of two algorithms. Given results can be implemented in aviation for flight control systems as well as other critical aviation information systems security ensuring [14].

Kiruba, et.al. (2018, May) - An IoT based health care application is implemented in real time and realized the application of IoT in health care. Next, the security aspects of the application has also been incorporated. LAAP protocol has been implemented to ensure authentication, anonymity and secure localization properties of the application. Data security is achieved by means of AES algorithm. Different modes of AES algorithm have been implemented and the impact of different modes of operation has been studied [15].

IV. CONCLUSION

In this survey cum comparative analysis of Securing Internet of Things (IoT) Devices AES vs Simon-Speck Encryptions discuss the different methods survey as well as shows comparison of different methods. Securing Internet of Things (IoT) devices is a critical concern in today's interconnected world. Encryption plays a vital role in ensuring the confidentiality and integrity of data transmitted between IoT devices and

the cloud or other endpoints. This paper gives the comparison of previous methods

V. REFERENCES

[1] "Survey of applications, advantages, and comparisons of AES encryption algorithm with other standards" Vol 2 , Issue 02, 22 March 2023.

[2] Rahul Neve, Dr. Rajesh Bansode, Vikas Kaul "Novel Lightweight Approach to Perform Cryptography for Data Security & Privacy in IoT Mobile Devices" ISSN:2147-67992147-16/July /2023.

[3] Baiq Yuniar Yustiarini; Favian Dewanta; Hilal Hudan Nuha "A Comparative Method for Securing Internet of Things (IoT) Devices: AES vs Simon-Speck Encryptions" 07 September 2022.

[4] L.Mary Shamala , Dr.G.Zayaraz , Dr.K.Vivekanandan, Dr.V.Vijayalakshmi "Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview" 2021.

[5] Pejman Panahi, Cüneyt Bayılmış, Unal Çavuşoğlu, Sezgin Kaçar "Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications" 13 January 2021.

[6] Abdulrazzaq H. A. Al-Ahdal1, Galal A. AL-Rummana, G.N. Shinde, Nilesh K. Deshmukh "NLBSIT: A New Lightweight Block Cipher Design for Securing Data in IoT Devices" 31 Oct 2020.

[7] Li Ning , Yasir Ali , Hu Ke, Shah Nazir, And Zhao Huanli "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things" 30, 2020.

[8] Chandel, Ankita, et al. "Comparative Analysis of AES & RSA Cryptographic Techniques."*2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. IEEE, 2019.

[9] Hafsa, Amal, et al. "A New security Approach to Support the operations of ECC and AES Algorithms on FPGA."*2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. IEEE, 2019.

[10] Ghosh, Pronab, et al. "A Variable Length Key Based Cryptographic Approach on Cloud Data."*2019 International Conference on Information Technology (ICIT)*. IEEE, 2019.

[11] Sönmez, Burcu, Ahmet Ali Sarıkaya, and Şerif Bahtiyar. "Machine Learning based Side Channel Selection for Time-Driven Cache Attacks on AES."*2019 4th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2019.

[12] Bhattacharjya, Aniruddha, Xiaofeng Zhong, and Xing Li. "A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack."*IEEE Access* 7 (2019): 30487-30506.

[13] Shvartsman, Phillip, and Xinmiao Zhang. "Side Channel Attack Resistant AES Design Based on Finite Field Construction Variation." 2019 IEEE International Workshop on Signal Processing Systems (SiPS). IEEE, 2019.

[14] Iavich, Maksim, et al. "Hybrid encryption model of AES and ElGamal cryptosystems for flight control systems." *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*. IEEE, 2018.

[15] Kiruba, W. Mercy, and M. Vijayalakshmi. "Implementation and Analysis of Data Security in a Real Time IoT Based Healthcare Application." *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2018.

[16] Mekki, Neila, et al. "A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system." *2018 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2018.

[17] Rachmawanto, Eko Hari, et al. "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator." *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE, 2018.

[18] Joshy, Amal, et al. "Text to image encryption technique using RGB substitution and AES." *2017 International Conference on Inventive Computing and Informatics (ICICI)*. IEEE, 2017.

[19] Adegbite, Oluwadara, and Syed Rafay Hasan. "A novel correlation power analysis attack on PIC based AES-128 without access to crypto device." *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2017.

[20] Balouch, Zaheer Abbas, Muhammad Imran Aslam, and Irfan Ahmed. "Energy efficient image encryption algorithm." *2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*. IEEE, 2017.

[21] Anup Ashok Patil, Shital Mali, "Hybrid Cryptography Mechanism for securing self-Organized Wireless Networks", IEEE, 2016.

[22] Raghav Mathur, Shruti Agarwal, Vishnu Sharma, "Solving Security Issues in Mobile Computing using Cryptography Techniques-A Survey", IEEE, 2015.

[23] Sánchez D, Batet M, Viejo A. "Utility-preserving sanitization of semantically correlated terms in textual documents." Inform Sci 2014;279:77–93.

[24] D. Zhang and H. Zhong, "A text hiding method using multiple-base notational system with high embedding capacity," Proc. of IEEE CISP, 2014

[25] Sánchez D, Batet M, Viejo A. "Automatic general-purpose sanitization of textual documents". IEEE Trans Inform Forensics Secur 2013;8:853– 62.

[26] Pranay Yadav, Sweta Maurya, Shilpi Sharma "Internet of Things based Air Pollution Penetrating System using GSM and GPRS" 2018.

[27] Pranay Yadav, Saima Khan, Sandeep Kumar Shukla "Design and Analysis of Modified Truncated Flexible T Shape Patch Antenna with DGS for 5G and IoT Application" 09-11 May 2022.

[28] Pranay Yadav, Alok Upadhyay, V. B. Surya Prasath, Zakir Ali, and Bharat Bhooshan Khare "Evolution of Wireless Communications with 3G, 4G, 5G, and Next Generation Technologies in India" volume 709, 2021.

[29] Ritu Shrivastava; Abhigyan Tiwary; Pranay Yadav "Challenges Block Chain Technology Using IOT for Improving Personal and Physical Safety – Review" 08-09 January 2021.

[30] Pranay Yadav, Shachi Sharma, Prayag Tiwari, Nilanjan Dey Amira S. Ashour and Gia Nhu Nguyen "A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max" 2018

[31] Pranay Yadav, Nishant Chaurasia, Kamal Kumar Gola, Vijay Bhasker Semwan, Rakesh Gomasta & Shivendra Dubey "A Robust Secure Access Entrance Method Based on Multi Model Biometric Credentials Iris and Finger Print" pp 315–331, 01 January 2023.

Cite this article as :

Sonam Rajput, Dr. Arvind Kaurav, Prof. Nehul Mathur, "A Literature Survey on Securing Internet of Things (IoT) Devices : AES vs Simon-Speck Encryptions", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 5, pp. 588-595, September-October 2023. Available at doi : https://doi.org/10.32628/IJSRST52310561

Journal URL : https://ijsrst.com/IJSRST52310561