International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# An Innovative Cryptography Safety Algorithm Called S-RSB-23 for Protecting Data Using Machine Learning Algorithm

**C. Bagath Basha[1], Dr. S. Rajaprakash[2], Dr. Nitisha Aggarwal[3], Dr. MD Riyazuddin[4], Mohd Sirajuddin[5], Srihari Babu Gole[6]**

**Submitted**: 16/07/2023 **Revised**: 07/09/2023 **Accepted**: 26/09/2023

**Abstract*:*** The modern world is dependent on information as a result of the fact that information is most compelling when presented in an open setting. The only judgements that could be made with this data concerned people's lives and the global financial market and were either good or negative. We need to be able to store, analyse, and organise the ever-increasing quantity of data that we are collecting on a daily basis since it will only continue to rise. These Twitter data will be analysed using Machine Learning Algorithms (MLA), which will also download them for further study. This data analysis does not provide dependable cryptographic techniques. In this study, we present the quick encryption technique S-RSB-23 and show how to transform the ASCII code to the corresponding hexadecimal value using this approach. The cells in this transformed code have been paired and then swapped. In comparison to the SALSA technique, the S-RSB-23 approach offers a much improved level of encryption throughput.

***Keywords:*** *Data, Twitter, MLA, SALSA, S-RSB-23*

## 1. Introduction

The present world relying upon the information bacause of this information is most impressive in open area. This data only made positive or negative decisions about people's lives and the global financial market.

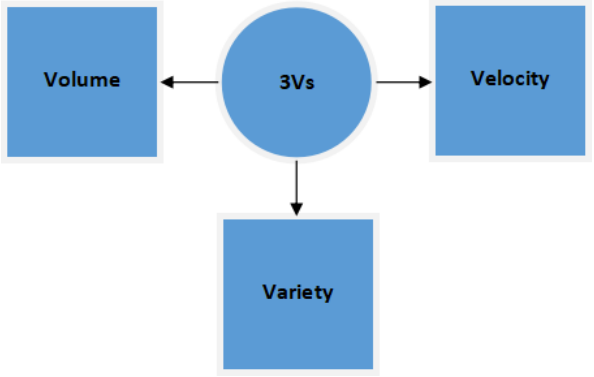

**Fig. 1.** Three V's data

Since the amount of data shown in Figure 1 will continue to grow, we must figure out how to store, process, and organize it. These information will be analzsed and downloaded from Twitter by MLA in Figure 2. The data that was analyzed did not yield any effective cryptographic algorithms.

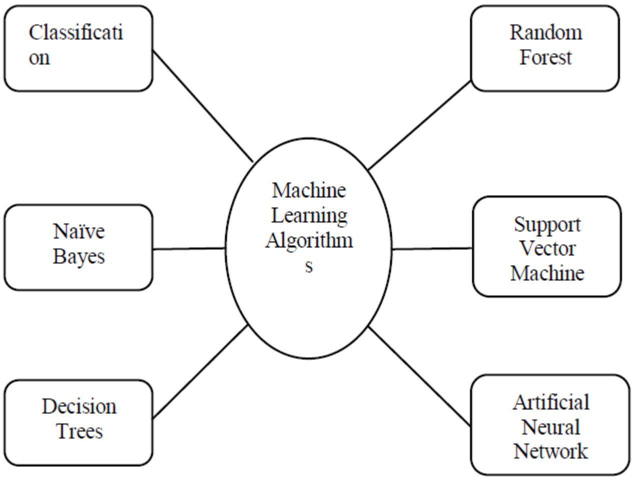

**Fig. 2.** Machine Learning Algorithms

The peculiarities of security need to be taken into account by important cryptographic algorithms. In 1949, Shannon saw diffusion and confusion as two fundamental qualities that were essential. The process of establishing a relationship between the ciphertext and the key is exceedingly difficult. The term "diffusion" refers to the practise of repeatedly using plaintext. These attributes serve as a portal via which the boolean functions of the cryptographic method may be accessed. This method is used to satisfy a number of criteria, one of which is strong nonlinearity. Other needs include algebraic degree features. This method was used for research on a technique

[1]*Department of CSE, Kommuri Pratap Reddy Institute of Technology, Autonomous, Hyderabad, Telangana, India.*
[2]*Department of CSE, Aarupadai Veedu Institute of Technology (AVIT),VMRF, Chennai, Tamil Nadu, India.*
[3]*Panipat Institute of Engineering and Technology, Samalkha, Haryana.*
[4]*Department. of Information Technology, Anurag University, Hyderabad, Telangana, India.*
[5]*Department of Information Technology, Vidya Jyothi Institute of Technology, Hyderabad, Telangana, India.*
[6]*Department of Information Technology, Anurag University, Hyderabad, Telangana, India.*
*chan.bagath@gmail.com[1], srajaprakash_04@yahoo.com[2], nitisha.cse@piet.co.in[3], riyaz.mdr1@gmail.com[4], mohd.siraj587@gmail.com[5], sriharibabug@gmail.com[6]*

called continuous diffusion analysis (CDA). The CDA is regarded as a probability for each bit, despite the fact that continuous bits may be flipped and modified with relative ease. Next, we will discuss the SALSA idea, which includes adding, rotating, and XORing series bits. This will follow the CDA discussion. The bits may be rotated in either the row or column directions. The AES algorithm includes this principle as one of its components. Encrypting and decrypting the code will take more time with this technique, despite the fact that it offers very high levels of security. As a direct consequence of this, we will be recommending a quick encryption method known as SALSA-RSB-23 (S-RajShaliniBagath-23).

The reaming the section will discuss as follows: In section II, the related work for machine learning and security. In section III, will discuss about the proposed methodology of the algorithm. In section IV, the explain the result mathematically and compare the methods through graphs and finally section V, the summarized the overall paper and advantage of the proposed method with future work.

## 2. Related Work

The CDA is a complicated statistical procedure, and the precise algorithmic implementation may be different depending on the software or programming language that is used. When doing CDA on empirical data, researchers often make use of specialised software programmes such as DMAT (Diffusion Model Analysis Toolbox) or fast-dm. These software packages provide researchers with the tools and functionalities necessary to carry out CDA [1]. The collecting and transmitting data, as well as interacting with a variety of different systems, are all activities that require establishing the optimal balance between the important factors of security and performance in the context of the Internet of Things (IoT). Because of this interconnectedness, there is an increased risk to data security as well as an increased difficulty in achieving desired levels of performance [2]. The utmost significance to protect nuclear power facilities from being attacked by hackers in order to guarantee the safety, dependability, and integrity of essential infrastructure. Methodologies of technical evaluation are put to use in nuclear power plants in order to analyse and put into place cyber security measures [3].

The procedure of presenting and analysing the findings of security tests conducted on a number of different projects and stages in a way that is both thorough and integrated. Visualising the discoveries, vulnerabilities, and overall security posture of web applications across a variety of projects and testing stages is a necessary part of this process [4]. The use of the potential of graphical models is one of the goals of this project, which intends to make cloud-based systems safer. Graphical models provide a method for representing complicated systems and the interactions between them in a graphical format. This kind of representation might be helpful for analysing and implementing security standards in cloud computing [5]. Defining security criteria, their applications, adoptions, and problems are all done with the help of the Common Criteria [6].

Smart environments that are built on the internet of things provide enormous prospects for enhancing productivity, automation, and convenience in a variety of settings, such as homes, cities, healthcare facilities, and industries. However, this leads to a huge increase in the number of security risks that need to be addressed. This article presents an in-depth analysis of the security standards and frameworks that have been established expressly for Internet of Things-based smart environments. By analysing the previously published material and the standard operating procedures of the industry [7]. The purpose of improving the safety of a distribution network. Depending on how close they are to potential security risks, it involves determining the level of security that various network components or nodes possess [8]. The process of putting into action a security protocol by using both a protocol trace and an ontology at the same time. This technique makes it possible to conduct an all-encompassing analysis of the security features of the protocol that is being implemented [9]. The implementation of risk entropy modelling as a method for assessing the possible dangers connected to the installation of surveillance cameras in public places is one way that might prove beneficial. It entails evaluating and measuring the many elements that contribute to the total risk level, taking into account both the good features (improved security) and the bad ones (concerns over privacy, improper use of data, etc.). [10]. The integration of Internet of Things (IoT) technology with power systems and infrastructure is referred to as the "Power IoT" [11]. At nuclear power plants, it is of the utmost importance to take all necessary precautions to protect sensitive digital assets. Even when there are already well-established cybersecurity systems in place, it is always to everyone's advantage to investigate new complementary points in order to improve the security measures [12]. Setting up an environment in which to simulate different attack scenarios and assess the security of Internet-of-Things (IoT) devices is one of the steps involved in the process of creating a security testbed for IoT devices [13]. SALSA, which stands for Scheduling Method for LoRa to LEO Satellites, is a scheduling method that was developed to handle communications between LoRa (long-range) devices and low-earth orbit (LEO) satellites in the most effective manner possible. Its purpose is to maximise the efficiency with which satellite resources are used and to reduce the likelihood of collisions occurring when many LoRa devices try to connect with one another at the same time [14]. Protecting data from social media platforms from unauthorized access while also preserving its confidentiality, integrity, and availability is an important part of data security. Algorithms that use machine learning have the potential to play a key role in the analysis and protection of data from social media platforms. Using machine learning algorithms to secure social media data may entail the following broad procedures and ideas [15]. Here are some generic stages and concepts that may be involved. There are a variety of tried-and-tested methods as well as standard operating procedures that are often used in order to make computers more secure [16]. The following are some broad approaches that may be used to improve the safety of computer systems. The purpose of this research is to analyse the sentiments expressed on Twitter data using a variety of machine learning algorithms and to do so within the context of big data. The algorithms that were chosen include conventional classifiers in addition to more sophisticated methods that are often used in natural language processing and sentiment analysis. The effectiveness of these algorithms will be evaluated using measures such as accuracy, precision, recall, and F1-score [17]. The use of blockchain technology in the healthcare business has the potential to revolutionise the industry by solving several difficulties relating to data security, interoperability, privacy, and trust. This might result in significant benefits for patients as well as providers. The following are some of the ways that blockchain technology is being used in the healthcare industry [18].They may have considerable advantages in terms of data security, integrity, interoperability, and analytics if they handle healthcare data. Let's dissect each component and investigate the ways in which they may cooperate to make healthcare data management more effective [19].Due to their potential to address issues with data integrity and security in computing settings, systems in the healthcare sector that use blockchain technology have recently attracted a lot of interest. Healthcare organisations have the capacity to improve data privacy, increase interoperability, and assure trustworthiness in their operations by embracing the decentralised and irreversible characteristics of blockchain technology. The following is an outline of how blockchain technology may be used in a healthcare system to guarantee the authenticity and safety of patient data [20-25].

They entail using the technology of cloud computing to store, manage, and process data and applications related to healthcare delivery. This strategy has several benefits over the more conventional on-premises solutions, such as increased scalability, flexibility, accessibility, and cost-effectiveness. The following are a few important facets of using cloud computing for the administration of healthcare [21].

## 2. Methodology

The technique S-RSB-23 that has been suggested involves first assigning the ASCII code for each bit, and then converting the resulting ASCII code to a hexadecimal number. Matrixes will be created using hexadecimal numbers as the basis. Each hexadecimal value will assign the cell number in matrices; the column wise rotation in the matrix will follow thereafter. Finally, switch the pair of hexadecimal numbers in Figure 3 to complete the process.

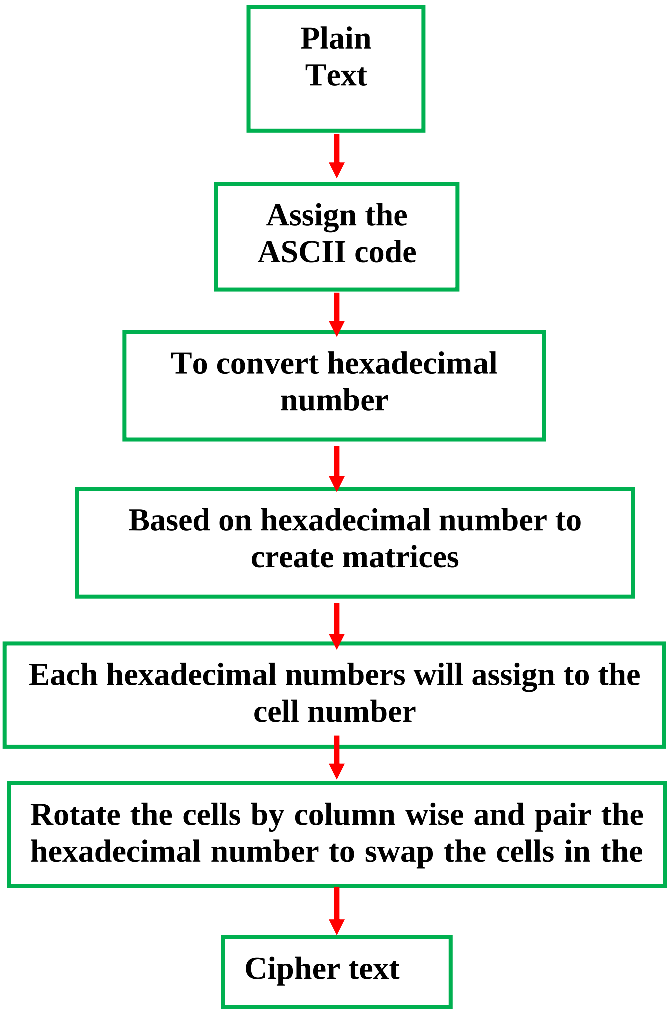
Plain Text
Assign the ASCII code
To convert hexadecimal number
Based on hexadecimal number to create matrices
Each hexadecimal numbers will assign to the cell number
Rotate the cells by column wise and pair the hexadecimal number to swap the cells in the
Cipher text

**Fig. 3.** S-RSB-23 Methodology

## 3. Algorithm

Step-1: Plain Text: HELLOWORLD

Step-2: Apply The ASCII Code For Plain Text.

Step-3: Convert To Binary Code From ASCII Code or Decimal Number in Table 1.

Step-4: Convert To Hexadecimal from binary code in Table 2.

Step 4: Each hexadecimal number will assign cell number in matrix.

Step 5: Rotate the cells by column wise in matrix.

Step 6: Pair the hexadecimal numbers and swap it.

**Table 1.** Plain text to ASCII code

| **LETTERS** | **ASCII CODE** |
|---|---|
| H | 072 |
| E | 069 |
| L | 076 |
| L | 076 |
| O | 079 |
| W | 087 |
| O | 079 |
| R | 082 |
| L | 076 |
| D | 068 |

**Table 2.** Plain text to ASCII code

| **ASCII Code** | **Binary Number** | **Hexa Decimal Number** |
|---|---|---|
| 072 | 01001000 | 48 |
| 069 | 01000101 | 45 |
| 076 | 01001100 | 4C |
| 076 | 01001100 | 4C |
| 079 | 01001111 | 4F |
| 087 | 01010111 | 57 |
| 079 | 01001111 | 4F |
| 082 | 01010010 | 52 |
| 076 | 01001100 | 4C |
| 068 | 01000100 | 44 |

## 4. Result & Discussion

S-RSB-23= $\begin{bmatrix} RSB0 & RSB1 & RSB2 & RSB3 \\ RSB4 & RSB5 & RSB6 & RSB7 \\ RSB8 & RSB9 & RSB10 & RSB11 \\ RSB12 & RSB13 & RSB14 & RSB15 \end{bmatrix}$

- To assign the hexadecimal numbers for each cell in matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB145 & RSB24C & RSB34C \\ RSB44F & RSB557 & RSB64F & RSB752 \\ RSB84C & RSB944 & RSB10 & RSB11 \\ RSB12 & RSB13 & RSB14 & RSB15 \end{bmatrix}$$

- To rotate the cells by column wise.
- Here second column cells are rotated, second cell move to the first cell, third cell move to the second cell, fourth cell move to the third cell, and first cell move to the fourth cell.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB24C & RSB34C \\ RSB44F & RSB944 & RSB64F & RSB752 \\ RSB84C & RSB13 & RSB10 & RSB11 \\ RSB12 & RSB145 & RSB14 & RSB15 \end{bmatrix}$$

- Similarly, third column cells are rotated, third cell move to the first cell, fourth cell move to the second cell, first cell move to the third cell, and second cell move to the fourth cell.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB34C \\ RSB44F & RSB944 & RSB14 & RSB752 \\ RSB84C & RSB13 & RSB24C & RSB11 \\ RSB12 & RSB145 & RSB64F & RSB15 \end{bmatrix}$$

- Similarly, fourth column cells are rotated, fourth cell move to the first cell, first cell move to the second cell, second cell move to the third cell, and third cell move to the fourth cell.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB44F & RSB944 & RSB14 & RSB34C \\ RSB84C & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To pair the hexadecimal numbers are 48,45,4C,4C,4F,57,4F,52,4C, and 44**.**
- To swap (4,8) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB84C & RSB944 & RSB14 & RSB34C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,5) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB944 & RSB84C & RSB14 & RSB34C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,C-3) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB944 \\ RSB15 & RSB84C & RSB14 & RSB34C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,C-3) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB944 & RSB84C & RSB14 & RSB34C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,F-6) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB14 & RSB84C & RSB944 & RSB34C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (5,7) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB14 & RSB34C & RSB944 & RSB84C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,F-6) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB10 & RSB15 \\ RSB944 & RSB34C & RSB14 & RSB84C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (5,2) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB34C & RSB15 \\ RSB944 & RSB10 & RSB14 & RSB84C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,C-3) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB34C & RSB944 \\ RSB15 & RSB10 & RSB14 & RSB84C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

- To swap (4,4) in the matrix.

S-RSB-23=

$$\begin{bmatrix} RSB048 & RSB557 & RSB34C & RSB944 \\ RSB15 & RSB10 & RSB14 & RSB84C \\ RSB44F & RSB13 & RSB24C & RSB752 \\ RSB12 & RSB145 & RSB64F & RSB11 \end{bmatrix}$$

**Table 3.** Salsa with S-RSB-23 encryption performance

| File Size | SALSA | S-RSB-23 |
|---|---|---|
| FS14 | 1.9 | 4.9 |
| FS66 | 2.3 | 5.1 |
| FS302 | 2.5 | 5.3 |
| FS812 | 3.3 | 5.5 |
| FS1521 | 3.6 | 5.8 |
| FS6570 | 4.2 | 6.1 |

The size of the file FS14 is three matrices; similarly, FS66 contains six matrices, FS302 contains ten, FS812 contains fifteen, FS1521 contains twenty, and FS6570 has forty. These numbers may be found in Table 3.

**Table 4.** ChaCha with S-RSB-23 encryption performance

| File Size | ChaCha | S-RSB-23 |
|---|---|---|
| FS14 | 1.7 | 4.9 |
| FS66 | 2.1 | 5.1 |
| FS302 | 2.2 | 5.3 |
| FS812 | 2.9 | 5.5 |
| FS1521 | 3.3 | 5.8 |
| FS6570 | 4.1 | 6.1 |

**Table 5.** S-RSB-23 encryption performance

| File Size | SALSA | ChaCha | S-RSB-23 |
|---|---|---|---|
| FS14 | 1.9 | 1.7 | 4.9 |
| FS66 | 2.3 | 2.1 | 5.1 |
| FS302 | 2.5 | 2.2 | 5.3 |
| FS812 | 3.3 | 2.9 | 5.5 |
| FS1521 | 3.6 | 3.3 | 5.8 |
| FS6570 | 4.2 | 4.1 | 6.1 |

The cryptographic power of ChaCha as well as the recommended methods need to be examined according to the degree to which they are resistant to assault. Known as one of the most secure stream cyphers available, ChaCha is resistant to a wide variety of cryptographic assaults. For the purpose of ensuring that the suggested approach offers an equivalent degree of protection, it needs to be subjected to intensive research and testing. Because ChaCha is intended to be a quick encryption method, it is well-suited for use in contexts in which speed is of the utmost importance. It makes use of elementary processes including additions, rotations, and XOR operations, all of which are easily implementable in either hardware or software and are outlined in Tables 4 and 5, respectively.

In particular, if the suggested approach intends to either supersede or perform better than ChaCha, it needs to strive for speeds at least equivalent to those of ChaCha or for speeds that are faster yet. When discussing encryption and decryption, the term "efficiency" refers to the number of computer resources needed for each process. Both ChaCha and Salsa are noted for their high levels of efficiency owing to the simplicity of their operations and their ability to be parallelized. Memory utilisation, power consumption, and hardware requirements are some of the aspects that should be taken into consideration while developing the suggested approach, which should aim for effective resource utilisation. Figures 4 and 5 highlight these factors.

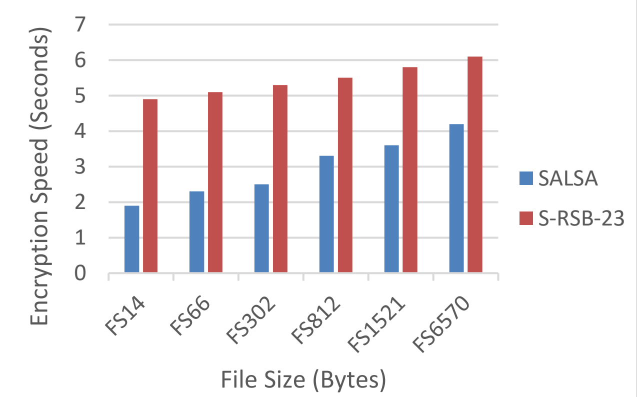

**Fig. 4.** Salsa vs S-RSB-23 Encryption performance

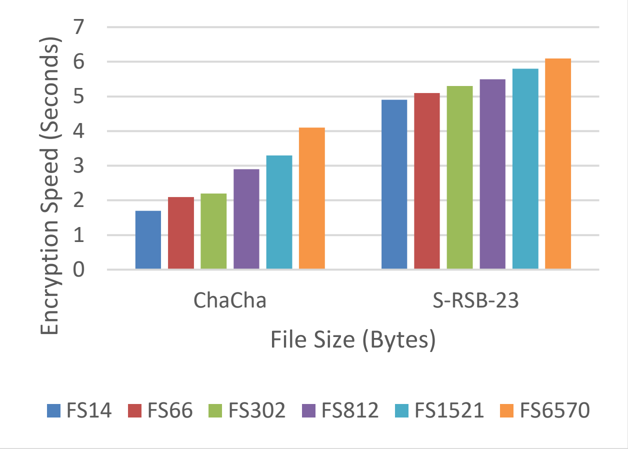

**Fig. 5.** ChaCHa vs S-RSB-23 Encryption performance

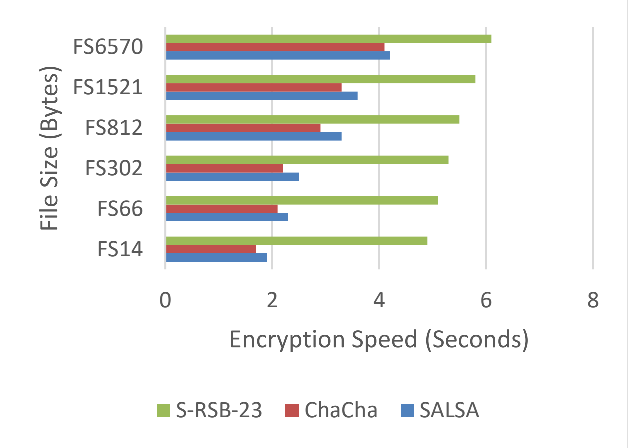

**Fig. 6.** S-RSB-23 Encryption performance

According to Figure 6, the S-RSB-23 technique was compared to the current approach in terms of how quickly encryption could be performed. The results of this comparison revealed that the suggested method performed much better, with times of 4.9, 5.1, 5.3, 5.5, 5.8, and 6.1 seconds, respectively. In comparison to the approach that is currently being used, the S-RSB-23 method offers much faster encryption.

## 5.Conclusion

In today's environment, people all over the globe depend heavily on information as a consequence of the fact that information is the most effective weapon in open space. Only judgements pertaining to people's lives and the international stock market were made using this data. This is one of the factors that contributes to the daily growth of data. This information does not supply strong cryptographic computations; thus, we developed the rapid encryption approach known as S-RSB-23. This technique converts the ASCII code to the corresponding hexadecimal value. The cells in this transformed code have been coupled with one another and switched around. When it comes to encrypting data, the S-RSB-23 approach is far more efficient than the SALSA method. The future work will add prime numbers and convert to the hexadecimal number.

## References

[1] M. Coutinho, R. T. De Sousa and F. Borges, "Continuous Diffusion Analysis," in IEEE Access, vol. 8, pp. 123735-123745, 2020, doi: 10.1109/ACCESS.2020.3005504. [1main]

[2] L. E. Kane, J. J. Chen, R. Thomas, V. Liu and M. Mckague, "Security and Performance in IoT: A Balancing Act," in IEEE Access, vol. 8, pp. 121969-121986, 2020, doi: 10.1109/ACCESS.2020.3007536.[2main]

[3] D. Jung, J. Shin, C. Lee, K. Kwon and J. T. Seo, "Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology," in IEEE Access, vol. 11, pp. 15229-15241, 2023, doi: 10.1109/ACCESS.2023.3244991.

[4] F. Ö. Sönmez and B. G. Kiliç, "Holistic Web Application Security Visualization for Multi-Project and Multi-Phase Dynamic Application Security Test Results," in IEEE Access, vol. 9, pp. 25858-25884, 2021, doi: 10.1109/ACCESS.2021.3057044.

[5] S. An, A. Leung, J. B. Hong, T. Eom and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," in IEEE Access, vol. 10, pp. 75117-75134, 2022, doi: 10.1109/ACCESS.2022.3190545.

[6] N. Sun et al., "Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges," in IEEE Access, vol. 10, pp. 44756-44777, 2022, doi: 10.1109/ACCESS.2022.3168716.

[7] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[8] J. Xiao, B. Zhang and F. Luo, "Distribution Network Security Situation Awareness Method Based on Security Distance," in IEEE Access, vol. 7, pp. 37855-37864, 2019, doi: 10.1109/ACCESS.2019.2906779.

[9] X. He, J. Liu, C. -T. Huang, D. Wang and B. Meng, "A Security Analysis Method of Security Protocol Implementation Based on Unpurified Security Protocol Trace and Security Protocol Implementation Ontology," in IEEE Access, vol. 7, pp. 131050-131067, 2019, doi: 10.1109/ACCESS.2019.2940512.

[10] H. Zhang, P. Li, Z. Du and W. Dou, "Risk Entropy Modeling of Surveillance Camera for Public Security Application," in IEEE Access, vol. 8, pp. 45343-45355, 2020, doi: 10.1109/ ACCESS. 2020.2978247.

[11] C. Choi and J. Choi, "Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service," in IEEE Access, vol. 7, pp. 110510-110517, 2019, doi: 10.1109/ACCESS.2019.2933859.

[12] J. Son, J. Choi and H. Yoon, "New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants," in IEEE Access, vol. 7, pp. 78379-78390, 2019, doi: 10.1109/ACCESS.2019.2922335.

[13] S. Siboni et al., "Security Testbed for Internet-of-Things Devices," in IEEE Transactions on Reliability, vol. 68, no. 1, pp. 23-44, March 2019, doi: 10.1109/TR.2018.2864536.

[14] M. Afhamisis and M. R. Palattella, "SALSA: A Scheduling Algorithm for LoRa to LEO Satellites," in IEEE Access, vol. 10, pp. 11608-11615, 2022, doi: 10.1109/ACCESS.2022.3146021.

[15] Batcha, B.B.C., Singaravelu, R., Ramachandran, M. et al., “A Novel Security Algorithm RPBB31 for Securing the Social Media Analyzed Data using Machine Learning Algorithms”, Wireless Pers. Commun., 2023, doi: https://doi.org/10.1007/s11277-023-10446-9

[16] Bagath Basha C and Rajapraksh S, “Enhancing The Security Using SRB18 Method of Embedding Computing”, Microprocessor and Microsystems, 2020.

[17] Bagath Basha C and Somasundaram K., “A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data”, International Journal of Recent Technology and Engineering, pp. 591-599, 2019.

[18] K Shantha shalini and M Nithya published a paper entitled, “A survey on adoption of blockchain in healthcare” in the International Journal of Business Intelligence and Data Mining (ISSN 1743-8195) on November 2022, Vol. 22, No. 1/2, 2023.

[19] K Shantha shalini and M Nithya published a paper entitled, “An Integrated approach of Block chain Technology with Machine learning and Cloud computing for handling healthcare data” in the International Journal of Health Sciences (ISSN 2550-6978) on May 2022,Special Issue-I.

[20] K Shantha shalini and M Nithya published a paper entitled “Block chain Based Healthcare System to Ensure Data Integrity and Security in Computing Environments” in the Journal of Green Engineering

(ISSN: 2245-4586) on November 2020, Volume-10, Issue-11.

[21] Yaseen, M., Hayder Sabah Salih, Mohammad Aljanabi, Ahmed Hussein Ali, & Saad Abas Abed. (2023). Improving Process Efficiency in Iraqi universities: a proposed management information system. Iraqi Journal For Computer Science and Mathematics, 4(1), 211–219. https://doi.org/10.52866/ijcsm.2023.01.01.0020

[22] Aljanabi, M. ., & Sahar Yousif Mohammed. (2023). Metaverse: open possibilities. Iraqi Journal For Computer Science and Mathematics, 4(3), 79–86. https://doi.org/10.52866/ijcsm.2023.02.03.007

[23] Atheel Sabih Shaker, Omar F. Youssif, Mohammad Aljanabi, ABBOOD, Z., & Mahdi S. Mahdi. (2023). SEEK Mobility Adaptive Protocol Destination Seeker Media Access Control Protocol for Mobile WSNs. Iraqi Journal For Computer Science and Mathematics, 4(1), 130–145. https://doi.org/10.52866/ijcsm.2023.01.01.0011

[24] Hayder Sabah Salih, Mohanad Ghazi, & Aljanabi, M. . (2023). Implementing an Automated Inventory Management System for Small and Medium-sized Enterprises. Iraqi Journal For Computer Science and Mathematics, 4(2), 238–244. https://doi.org/10.52866/ijcsm.2023.02.02.021

[25] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2167

[26] Naga Swetha, G. ., & M. Sandi, A. . (2023). A Brand-New, Area - Efficient Architecture for the FFT Algorithm Designed for Implementation of FPGAs. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 114–122. https://doi.org/10.17762/ijritcc.v11i2.6135

[27] Isabella Rossi, Reinforcement Learning for Resource Allocation in Cloud Computing , Machine Learning Applications Conference Proceedings, Vol 1 2021.