MSRDG International Journal of Computer Scientific Technology & Electronics Engineering ISSN: 3107 - 426X
Volume 1 Issue 4, 1-7, August 2025

To Apply the SRow Operations for Improve the Security of Cloud-Based Data

K. Karthik[1], Prabhu Rengaramanujam[2] , A. Manikandan[3]

[1]*Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation (DU), Chennai, Tamil Nadu, India.*
[2]*Senior Engineer, Guidewire Software Inc., USA.*
[3]*HCL Technologies, 31 International Park, Singapore.*
[1]*karthik@avit.ac.in*

Abstract - *The Internet of Things (IoT) shows a new way to create heterogeneous and distributed systems that can be used as a platform for ubiquitous computing services. Because the Internet of Things (IoT) creates so much data that there aren't enough processing and storage resources to handle it all, a cloud-based architecture is being employed a lot to meet these needs. As a result, the cloud-based Internet of Things ecosystem has had a lot of serious security and trust problems. To address these challenges, a new strategy called SRow operations has been put forward. The approach has four different parts. 1. Choose the Secret Message— Pick a message that you want to keep private. 2. To apply the ASCII code for secret message. 3. To swap the cell values in the matrix using encrpted secret message. 4. you will exchange the row operations in the matrix. Plain text is changed into encrypted text to protect the information. To decrypt something, you have to undo the conversion, which gives you the message in its original form. The suggested solution is safer than other common ways of encrypting data.*

Keywords - *ChaCha, decryption, encryption, performance, SRow*

1. Introduction

The fast-growing Internet of Things (IoT) connects physical objects via embedded electronics, software, sensors, and network connections. Devices, cars, buildings, and intelligent systems are examples. This network ensures that data collected and transferred regularly between people and their devices is consistent. Internet of Things devices have limited computational power and storage, thus complex processing and large-scale data management are offloaded to cloud services. The Internet of Things is crucial in modern technology because it improves efficiency, scalability, and system performance by connecting to the cloud. For instance, Internet of Things devices create massive amounts of data, which may strain networks. Cloud computing efficiently processes and stores this data, improving cloud-based Internet of Things system speed and scalability. Figure 1 demonstrates the architecture of a cloud-integrated IoT framework.

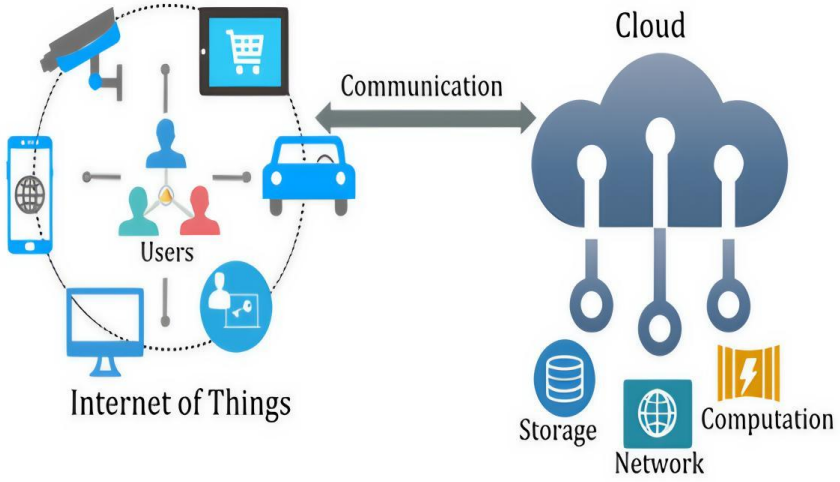

Fig.1 Environment of IoT.

IoT integration with cloud computing increases technological resources. However, cloud-based Internet of Things solutions, like many other emerging technologies, have challenges. Two major issues are safety. Therefore, shifting Internet of Things activities to the cloud necessitates transferring trust and security issues to cloud infrastructure. However, most Internet of Things security research focuses on wireless networks, and cloud-based trust assessment is scarce. This article improves cloud-based Internet of Things (IoT) security by analyzing cloud service trustworthiness utilizing security measures and reputation-based assessment.

2. Related work

The author discussed cloud security and mentioned four high-level concepts for governing alternative clouds [1]. Using the Internet of Things, the authors created a trustworthy cloud security solution and an efficient cloud computing service [2]. These writers created a cloud security strategy for the public and businesses [3]. After investigating four depth security approaches, the authors assessed depth cloud security [4]. The authors employ machine learning to improve social media data safety. This study adds to social media data protection literature [5]. The authors built a virtual cloud network (VCN) security architecture and evaluated which of the three clouds is more popular [6]. These authors propose deleting data, particularly third-party-contracted data [7]. This paper discusses how adversarial attacks might affect machine learning models and the urgent need for robust cryptographic approaches in AI-based security solutions [8]. The authors used cloud sensor architectures to study security threats [9]. They analyzed the various methods and are presently investigating the mechanisms provided for future verification [10]. This research investigates if multi-path routing can improve distributed ledger transaction safety and efficiency. focused on optimizing encrypted data transmission via blockchain nodes [11]. They are researching stakeholder safety to advance e-health research [12]. The authors studied 67 fields, although they focused on support vector machines (SVM) in machine learning [13]. The authors investigated mobile device cloud computing capabilities [14] to ensure healthcare security. This article discusses cryptographic methods designed to secure large amounts of data in cloud and distributed environments [15]. This article discusses cryptography. The Secret Row Operations (SRow) approach was proposed after reviewing the literature.

3. Methodology

SRow Operations suggested approach consists of four different processes. *1. Choose the Secret Message— Pick a message that you want to keep private. 2. To apply the ASCII code for secret message. 3. To swap the cell values in the matrix using encrpted secret message. 4. you will exchange the row operations in the matrix* are shown in Figure 2.

Encryption Process

- Select the secret message: Pick a key to encrypt.
- To apply the ASCII code for secret message.
- To swap the cell values using a secret key in the matrix.
- Apply the row operations in the matrix.

4. Result & Discussion

$$PT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{14} \\ NC_{21} & NC_{22} & NC_{23} & NC_{24} \\ NC_{31} & NC_{32} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

- Plain Text = Diamond
- PT = 68736577797868

1ST process (6,8)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{14} \\ NC_{21} & NC_{22} & NC_{31} & NC_{24} \\ NC_{23} & NC_{32} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

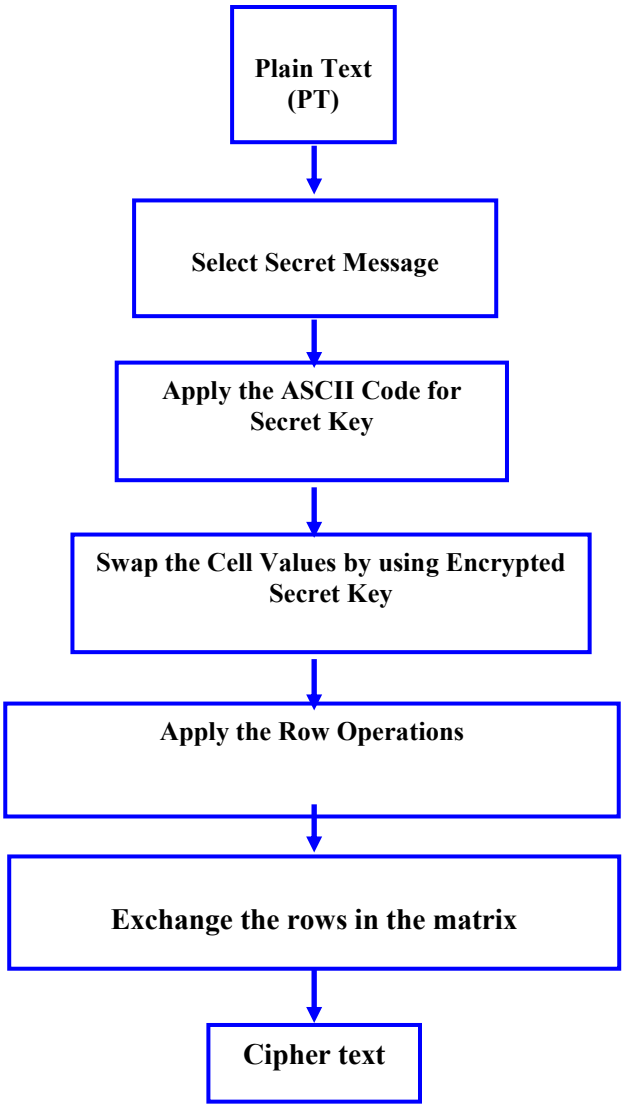

Fig. 2 SRow Operation Methodology

2nd process (7,3)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{22} & NC_{31} & NC_{14} \\ NC_{23} & NC_{32} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

3rd process (6,5)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{31} & NC_{22} & NC_{14} \\ NC_{23} & NC_{32} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

4th process (7,7)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{31} & NC_{22} & NC_{14} \\ NC_{23} & NC_{32} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

5th process (7,9)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{31} & NC_{22} & NC_{32} \\ NC_{23} & NC_{14} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

6th process (7,8)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{31} & NC_{22} & NC_{23} \\ NC_{32} & NC_{14} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

7th process (6,8)

$$RT = \begin{bmatrix} NC_{11} & NC_{12} & NC_{13} & NC_{24} \\ NC_{21} & NC_{31} & NC_{32} & NC_{23} \\ NC_{22} & NC_{14} & NC_{33} & NC_{34} \\ NC_{41} & NC_{42} & NC_{43} & NC_{44} \end{bmatrix}$$

- To apply the row operations

1st process to exchange the first and last rows

$$RT = \begin{bmatrix} NC_{41} & NC_{42} & NC_{43} & NC_{44} \\ NC_{21} & NC_{31} & NC_{32} & NC_{23} \\ NC_{22} & NC_{14} & NC_{33} & NC_{34} \\ NC_{11} & NC_{12} & NC_{13} & NC_{24} \end{bmatrix}$$

2nd process to exchange the second and third rows

$$RT = \begin{bmatrix} NC_{41} & NC_{42} & NC_{43} & NC_{44} \\ NC_{22} & NC_{14} & NC_{33} & NC_{34} \\ NC_{21} & NC_{31} & NC_{32} & NC_{23} \\ NC_{11} & NC_{12} & NC_{13} & NC_{24} \end{bmatrix}$$

Table 1. SRow operations encryption performance

File Size (Bytes)	ChaCha	Salsa	SRow
55	1.21	1.09	1.6
89	1.49	1.24	2
166	1.99	1.85	2.3
256	2.03	2.4	3.1
345	2.44	2.6	3.7

This link opens Table 1, which compares the three encryption speeds. SRow operations, a unique methodology owing to its essential properties, provides a faster speed performance than other methods. SRow operations, a new technique, outperforms competitors like the “ChaCha” method in Figure 3, “Salsa” method in Figure 4 and “SRow” method in Figure 5 with performance rates of 1.6, 2, 2.3, 3.1, and 3.7 milliseconds.

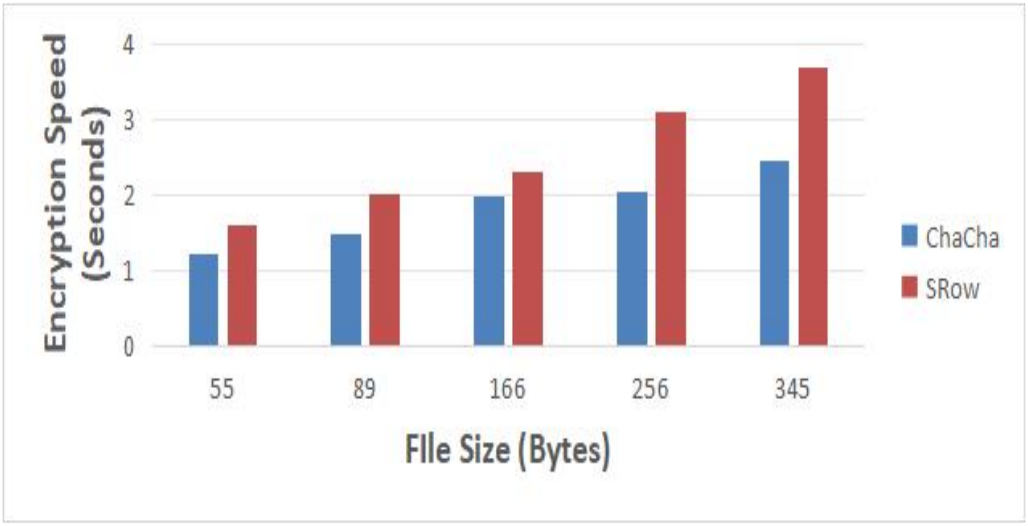

Fig. 3 ChaCha Vs SRow Encryption Speed

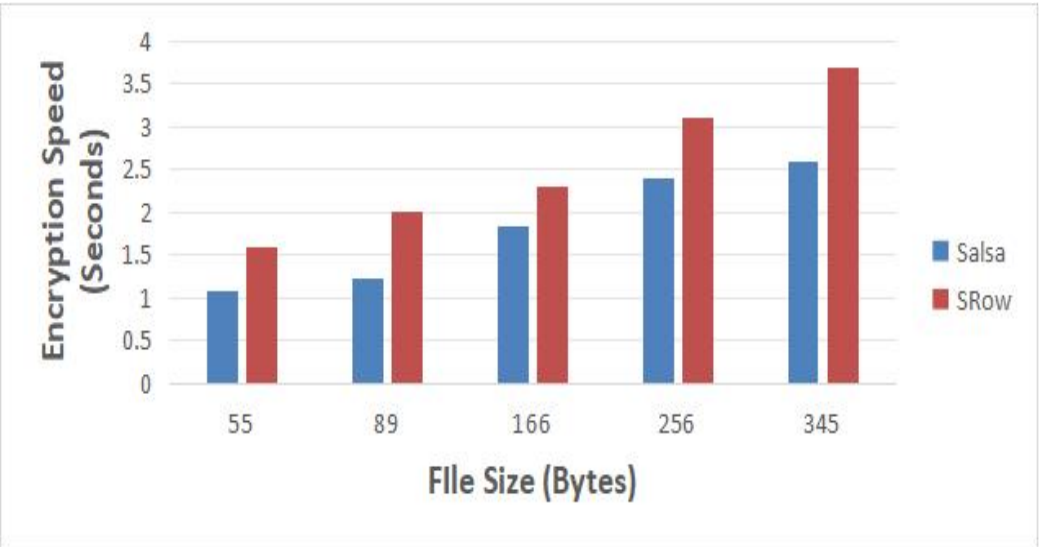

Fig. 4 Salsa Vs SRow Encryption Speed

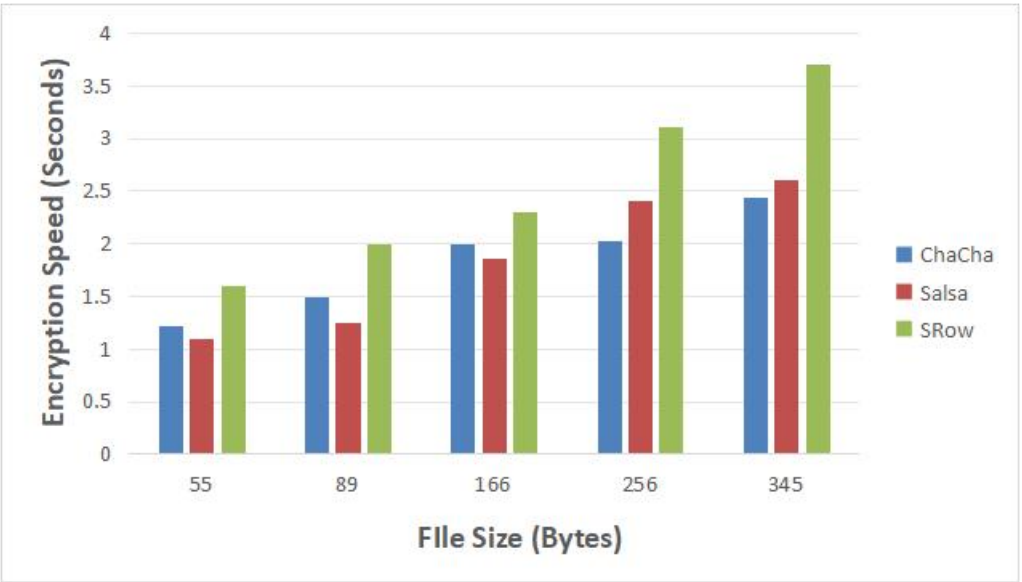

Fig. 5 ChaCha Vs Salsa Vs SRow Encryption Speed

5. Conclusion

The Internet of Things (IoT) offers a new way to build large, distributed systems that may be utilized for computing services anywhere. Cloud-based architectures are employed when there are not enough computers and storage space to handle the massive amounts of IoT data. Thus, cloud-based Internet of Things has several trust and security issues. SRow operations addresses these challenges with a new method. This procedure comprises two steps.1. Choose the Secret Message— Pick a message that you want to keep private. In the second stage, you will exchange the row operations in the matrix. The proposed method provides higher security than standard encryption.

References

[1] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 523-536, 1 July-Sept. 2017, doi: 10.1109/TCC.2015.2415794.

[2] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach", in IEEE Access, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[3] K. P. Joshi, L. Elluri and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance", in IEEE Access, vol. 8, pp. 148541-148555, 2020, doi: 10.1109/ACCESS.2020.3008964.

[4] 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.

[5] 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., pp. 581–608, 2023.

[6] J. Deng et al., "A Survey on Vehicular Cloud Network Security", in IEEE Access, vol. 11, pp. 136741-136757, 2023, doi: 10.1109/ACCESS.2023.3339192.

[7] C. Yang, Y. Liu, X. Tao and F. Zhao, "Publicly Verifiable and Efficient Fine-Grained Data Deletion Scheme in Cloud Computing", in IEEE Access, vol. 8, pp. 99393-99403, 2020, doi: 10.1109/ACCESS.2020.2997351.

[8] Basha, C. B. ., Rajaprakash, S. ., Aggarwal, N. ., Riyazuddin, M. ., Sirajuddin, M. ., & Gole, S. B. . (2023). An Innovative Cryptography Safety Algorithm Called S-RSB-23 for Protecting Data Using Machine Learning Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 12(2s), pp. 503–510, 2024.

[9] R. Alturki et al., "Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks", in IEEE Access, vol. 9, pp. 89344-89359, 2021, doi: 10.1109/ACCESS.2021.3088225.

[10] K. Muniasamy, R. Chadha, P. Calyam and M. Sethumadhavan, "Analyzing Component Composability of Cloud Security Configurations", in IEEE Access, vol. 11, pp. 139935-139951, 2023, doi: 10.1109/ACCESS.2023.3340690.

[11] C. Bagath Basha, S. Rajaprakash, Nitisha Aggarwal, MD Riyazuddin, G. Sujatha, K. Karthik, "The Design of Security Algorithm RPBB-24-1 in Multi-Way Path over the Distributed Ledger," SSRG International Journal of Electrical and Electronics Engineering, vol. 11, no. 4, pp. 36-44, 2024. https://doi.org/10.14445/23488379/IJEEE-V11I4P105.

[12] A. Sahi, D. Lai and Y. Li, "A Review of the State of the Art in Privacy and Security in the eHealth Cloud", in IEEE Access, vol. 9, pp. 104127-104141, 2021, doi: 10.1109/ACCESS.2021.3098708.

[13] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review", in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[14] M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing", in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[15] S Rajaprakash, C Bagath Basha , S Muthuselvan , N Jaisankar and Ravi Pratap Singh, "RBJ25 cryptography algorithm for securing big data", Journal of Physics: Conference Series, 2020.