

A cellular automata approach for extending data privacy and security of edge computing

Sandeep Kumar Sharma *

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Anil Kumar [†]

Department of Computer Science and Engineering

Poornima Institute of Engineering and Technology

Jaipur

Rajasthan

India

Abstract

This article introduces a cellular automaton (CA) based method to heighten the security breach of edge computing data. Edge computing is an innovative computing paradigm that controls the processing network's edge devices. Relocating computation nearer to the resource is the main goal of edge computing. Based on the CA's concept, a strong secret key is introduced for text cryptography. The secret key generated in this research is a 64-character key, which performs substitutions and reverse substitutions on the plain text and cipher text by dividing the text into blocks of 64 characters. The key may be to use the same or different letters to substitute the same letters of the plain text which makes it a unique key. The strength of the key is evaluating using the substitution speed, memory utilization, possible attack, and avalanche effects.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Edge computing, Cellular automata, Transition function, Neighborhoods, Privacy and security, Cryptography key.

* E-mail: dr.sks.cs@gmail.com (Corresponding Author)

† E-mail: anil.vashu@gmail.com

1. Introduction

Technology has become a part of many sectors and people's everyday lives because of the growth of real-time applications and the ongoing improvement of society's needs. Edge computing has wedged every section of such applications, involving intelligent inventing, smart homes, autonomous vehicles, and the transportation sector. As per the cloud global index, the Internet has billions of shareable devices that generate vast amounts of data [1]. Generally, cloud computing stores and processes that data, which may lead to issues, i.e., high-risk, limited control, internet connectivity, etc. For example, smartphone applications are operated using cloud computing and will ask for user information, ask for access to mobile storage, and monitor user activity when utilizing their various applications. When uploading the user data to the cloud, there is a considerable danger of privacy trickle or assault on the data. The service provider owns the operation and execution of services within a cloud infrastructure, and users have less control over accessing the cloud data [2].

Edge computing is a novel paradigm that manages the computing of the local network, as compared to conventional cloud computing. The primary aim of edge computing is to relocate computation nearer to the source of the data [3]. To put it another way, edge computing is the process of creating data and carrying out computations at the control of the edge network. Edge computing requires shifting the network, data, storage, resources, and processing capabilities to the control of the network to satisfy the demands of the IT sector [4]. To meet the high bandwidth and low latency requirements of the web, it also offers services at the edge network devices. However, edge computing cannot replace the function of the cloud. The cloud is enhanced by edge computing, and the two technologies offer incredible performance for particular use cases [5].

In a distributed IT architecture known as edge computing, computing resources are moved from clouds and data centers to locations as close as possible to the source. The key objectives of edge computing are to reduce latency requirements while processing data and lower network expenses. In another way, edge computing states the establishment of services and computations at the network and data creation limits. The digital transforms will be greatly aided by the coexistence, complementarity, and coordinated development of edge and cloud computing in the domains of network, business, application, and intelligence [6]. To accomplish in-depth research and produce more insightful analysis findings, all data

onto edge nodes still need to be summarised in the cloud. As a result, cloud computing continues to be crucial to the advancement of increasingly intelligent Internet of Things devices. From the perspective of the Internet of Things, cloud computing will result in a substantial liability if the vast quantity of data produced by the linked devices is sent there. Currently, edge computing is needed to share the load from the cloud and handle tasks that fall within its area of expertise. The data in the cloud is not lost in the event of an edge computing issue [7].

To handle certain Internet services like in-depth data mining and sharing some data must first be processed by edge computing and then returned to the cloud. This necessitates the collaboration of edge and cloud computing. The Internet of Things network's linked devices are made more stable by these two advancements [8].

Edge computing makes use of real-time features and, when combined with cloud computing and synergy, enhances production efficiency and the early detection of equipment faults. Edge computing nodes in the context of smart homes mostly comprise a few intelligent terminals. To achieve edge node management from the cloud and edge node access to the cloud, edge computing nodes compute heterogeneous data from various devices and upload it to the cloud for processing [9].

Edge computing appears with a few of privacy and data security issues that should be cautiously considered. The following are some of the most notable data security and privacy concerns related to edge computing [10]:

- Different data storage and localization laws may apply to data generated at the edge. It can be difficult to make sure that data is processed and kept by local rules and regulations, particularly when working with data that is transnational.
- Reliable encryption and decryption mechanisms are necessary for the transmission and storage of sensitive data at the edge. Data in transit or at rest may be susceptible to interception or unauthorized access if appropriate encryption is not used.
- Edge computing requires processing data, possibly sensitive and personal data, closer to the source. It is essential to make sure that personally identifiable information is handled appropriately and following privacy laws. In multi-stakeholder contexts, identifying who owns and has control over data created at the edge can be difficult. Disputes and possible data misuse can result from unclear ownership and control of data.

- It can be difficult to monitor and audit data flows and access at the edge. It becomes challenging to recognize and react to security problems quickly in the absence of adequate auditing and logging.

The proposed research focus is on enabling users to perform various operations (like inspecting, penetrating, encrypting, and decrypting) on data while ensuring the privacy of user's data because data will be stored and processed by entities that are not under the user's control [11]. To maintain integrity, the data are inspected before storing on the edge. To maintain authenticity, the encrypted copy of the data is also stored on the edge and time to time compared with the original data. To maintain confidentiality, only encrypted data are shared on the edge devices [12].

2. Cryptography Key Generation

An introduction to Cellular Automata (CA) theory is given in this section, which is followed by a discussion of cryptography key generation using CA. The term "cellular automata" describes discrete dynamical systems that function on a regular pattern of grids or cells which is either in one-dimensional or two-dimensional [14]. According to the CA, the cell's value represents the current state. With a modification to its value, the cell's present state was transformed into a new one. An automata's rule or transition function may serve as the basis for updating. The CA analysis the neighborhood cells and defines a transition function TF which may be applied to the current state CS of the cell and generate a new state NS, as equation 1 [15-16].

$$Cell_{NS} = TF(Cell_{CS}) \quad (1)$$

The cryptographic key of the proposed research has been generated with the help of two-dimensional CA. The cryptographic key generation process starts with selecting a text T. The text may be a group of sentences containing at least 64 characters. The stop words of the text should be removed, and the significant words should be stored in a data structure DS of the size 8*8. For each $Cell_{i,j}$ of the data structure DS, the internal operation is performed using equation 2. The detailed process of the key generation is depicting in the algorithm 1. The output of the algorithm is CK that works as a cryptographic key.

$$Cell_{i,j} = \frac{\sum_{x=i-1, y=j-1}^{x=i+1, y=j+1} Cell_{x,y}}{9} \quad (2)$$

Algorithm 1: Key generation

Input: Read a text of 64 or more characters.

Process:

Step 1: Remove stop words from the text.

Step 2: Select significant words.

Step 3: Store the significant words in a two-dimensional data structure of size 8*8.

Step 4: Each character of the 2D data structure is converted into a corresponding key.

Step 5: The alphabetic letters from a to z are assigned a key value i.e., 1 to 26.

Step 6: Expand the data structure by adding virtual cells with a value of 0 outside the data structure.

Step 7: For each $Cell_{i,j}$ of the data structure perform the following:

For $i=0, j=0$ to $i<8$ and $j<8$

$$SN_{i,j} = 0$$

For $x=i-1, y=j-1$ to $x\leq i+1$ and $y\leq j+1$

$$SN_{i,j} = SN_{i,j} + Cell_{x,y}$$

$$CK_{i,j} = \frac{SN_{i,j}}{9}$$

Example of cryptography key generation is depicted in the Figure 1. Consider the text of the key generation process is “Edge computing data security and privacy can be achieved by implementing cryptography concepts”. After removing the stop words, the significant words are {“Edge”, “computing”, “data”, “security”, “privacy”, “implementing”, “cryptography”, and “concepts”}. The significant words are stored in a data structure of 8*8 shown in Figure 1(a). The alphabetic keys 1 to-26 of the characters of significant words are depicted in Figure 1(b), expanded data structure and final cryptography key are depicted in the Figures 1(c) and 1(d) respectively.

e	d	g	e	c	o	m	p
u	t	i	n	g	d	a	t
a	s	e	c	u	r	i	t
y	p	r	i	v	a	c	y
i	m	p	l	e	m	e	n
t	i	n	g	c	r	y	p
t	o	g	r	a	p	h	y
c	o	n	c	e	p	t	s

1(a). Significant words

5	4	7	5	3	15	13	16
21	20	9	14	7	4	1	20
1	19	5	3	21	18	9	20
25	16	18	9	22	1	2	25
9	13	16	12	5	13	5	14
20	9	14	7	3	18	25	16
20	15	7	18	1	16	8	25
3	15	14	3	5	16	20	19

1(b). Alphabetic keys

0	0	0	0	0	0	0	0	0	0
0	5	4	7	5	3	15	13	16	0
0	21	20	9	14	7	4	1	20	0
0	1	19	5	3	21	18	9	20	0
0	25	16	18	9	22	1	2	25	0
0	9	13	16	12	5	13	5	14	0
0	20	9	14	7	3	18	25	16	0
0	20	15	7	18	1	16	8	25	0
0	3	15	14	3	5	16	20	19	0
0	0	0	0	0	0	0	0	0	0

1(c). Data structure expansion

6	7	7	5	5	5	8	6
8	10	10	8	10	10	13	9
11	15	13	12	11	9	11	9
9	14	12	12	12	11	12	8
10	16	13	12	10	10	13	10
10	14	12	9	10	10	16	10
9	13	11	8	10	12	18	13
6	8	8	5	7	7	12	8

1(d). Final cryptography key

Figure 1
Example of cryptography key generation

3. Data Security and Privacy Implementation

Edge computing, which processes data closer to the thrust of data initiation rather than depending exclusively on centralized cloud servers, raises important privacy and data security issues. For reducing latency and enhancing reaction times, edge computing processes data closer to the source. Susceptible data is nevertheless processed and kept locally on devices due to this closeness. To stop illegal access or manipulation, it is essential to protect this data. Users and associations should have faith that their data is controlled privately and securely. Determining a commitment to privacy and data security in edge computing fosters confidence, which is essential for these technologies to be widely used. Edge devices are susceptible to local attacks or physical exploitation. Strong data security protocols guarantee the confidentiality and integrity of the data processed and stored on edge devices, assisting in the improvement of these risks.

The proposed research invents a method for securely managing the data and maintaining data integrity while sharing with others. The proposed method creates a unique secret key to encrypt and decrypt the data. The secret key generated by the proposed method is a type of polyalphabetic and one-time padded substitute methods. The created secret key is a group of 64 characters arranged in 8*8 size of data structure. The text to be encrypted by the proposed method is also divided into a block of 64 characters of the same size. If number of characters are less than to 64 then a special character “#” to be added to those cells. The

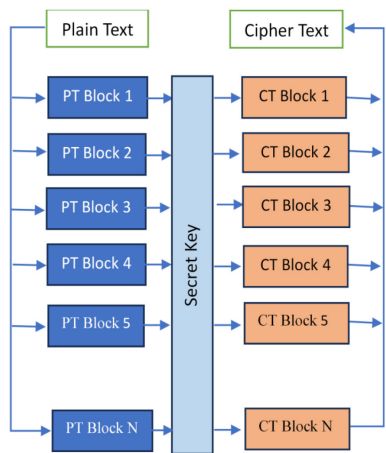


Figure 2

Encryption process of proposed methodology

process of data encryption of the proposed methodology is visualized in the Figure 2. The secret key converts the edge data called plain text into encrypted text called cipher text.

Algorithm 2: Text encryption and decryption

Input: Plain text PT and Secret key CK [8*8]

Process:

Step 1: Divide the plain text into N number of blocks of size 8*8.

$B = \{B_1, B_2, B_3, B_4, B_5, B_6, B_7, \dots B_N\}$

Step 2: If $\text{len}(B_N) < 64$

For $i = \text{len}(B_N)$ to 64

$B[i] = \text{'\#'}'$

Step 3: Set $D = \{ \text{'a':1, 'b':2, 'c':3, 'd':4, 'e':5, 'f':6, 'g':7, 'h':8, 'i':9, 'j':10, 'k':11, 'l':12, 'm':13, 'n':14, 'o':15, 'p':16, 'q':17, 'r':18, 's':19, 't':20, 'u':21, 'v':22, 'w':23, 'x':24, 'y':25, 'z':26, '\#':0} \}$

Step 4: Convert all the characters into keys as per D for all the blocks B.

Step 5: for $x=1$ to N

for $i=0$ to 7 and $j=0$ to 7

If $B_x[i][j] \neq 0$

$CT_x[i][j] = (B_x[i][j] + CK[i][j]) \bmod 26$

Step 6: Convert all the keys of CT_x into corresponding characters.

Step 7: Combine all cipher text blocks CT_x into a single block CT.

Step 8: To regenerate plain text from cipher text, repeat all the steps from 1 to 7 on cipher text with one difference. In step 5, + sign should be replaced with – sign.

$PT_x[i][j] = (CT_x[i][j] - CK[i][j]) \bmod 26$

The decryption process of the proposed methodology is performed using the same secret key with reverse substitutions. The working of the secret key with substitutions and reverse substitutions is depicted in algorithm 2. The algorithm accepts two parameters i.e., plain text PT and secret key CK generated by the key generation algorithm.

The proposed method provides confidentiality and integrity to any size of text data. The data could be stored securely and maintain privacy of the data while shared with other devices. The proposed method achieved its objectives by generating a strong secret key. A substitution

Table 1
Performance Evaluation

S. No	Performance Criteria	Outcome
1	Encryption and Decryption speed	Medium
2	Memory utilization	High
3	Possible attack	Known ciphertext attack
4	Avalanche Effect	Strong

method has been used to encrypt the data, but the prediction of the key is very difficult. Compared to basic substitution ciphers, the proposed approach is more intricate because it employs several substitution alphabets depending on a keyword. Attacks using frequency analysis may be less successful because of this intricacy.

To understand the strengths of the proposed methodology, we assume the text “Cryptography is the method of encrypting and decrypting a text” and same secret key should be used which has been generated in the second section of this article. Figure 3 demonstrate an example of the encryption process of the proposed methodology.

After applying the secret key on the plain text, the cipher text become “iyfuytoxizrg sf ewr xneqxr ar qvmhlbdslq kbp mnsbgceqxs m bmca”. As we analysis the substitutions, every time the same letter has been substituted with different letter and retrieving of such substitutions is very difficult. The performance of the proposed methodology is measured using encryption and decryption speed, memory utilization, possible types of attack, and avalanche effect. The cipher text should change significantly in response to a small change in either the plain text or the key, this feature is referred to as the “avalanche effect”. Table 1 represents the performance evaluation of the proposed methodology.

5. Discussion and Conclusion

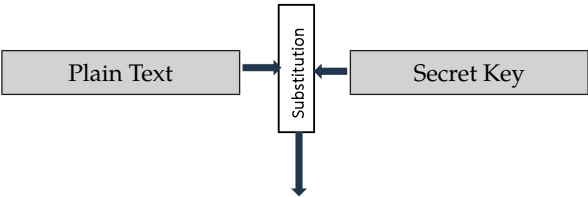
This paper introduced a novel method for providing security and privacy to the data of edge computing. The proposed method generates a strong secret key using a random text with the help of cellular automata concepts. The key can encrypt any size of text data by dividing it into blocks of 64 characters. A substitution approach has been used to convert plain text to cipher text and vice versa. The key uses the same or different letter if any letter is repeated many times. This concept helps to make a strong avalanche effect and makes the method unique. The encryption

c	r	y	p	t	o	g	r
a	p	h	y	#	i	s	#
t	h	e	#	m	e	t	h
o	d	#	o	f	#	e	n
c	r	y	p	t	i	n	g
a	n	d	#	d	e	c	r
y	p	t	i	n	g	#	a
#	t	e	x	t	#	#	#

Plain Text

6	7	7	5	5	5	8	6
8	10	10	8	10	10	13	9
11	15	13	12	11	9	11	9
9	14	12	12	12	11	12	8
10	16	13	12	10	10	13	10
10	14	12	9	10	10	16	10
9	13	11	8	10	12	18	13
6	8	8	5	7	7	12	8

Secret key



	i	y	f	u	y	t	o	x
	i	z	r	g	#	s	f	#
	e	w	r	#	x	n	e	q
	x	r	#	a	r	#	q	v
	m	h	l	b	d	s	l	q
	k	b	p	#	m	n	s	b
	g	c	e	q	x	s	#	m
	#	b	m	c	a	#	#	#

Encrypted Text

Figure 3
Example of plain text encryption using generated secret key

and decryption speed and memory utilization are also efficient as compared to other substitution methods. The retrieving of the secret key for the attackers is very difficult, they may have only known ciphertext attack to retrieve the plain text. The proposed method could be used to secure the data of cloud computing in the future scope.

References

- [1] Shalin Parikh, Dharmin Dave, Reema Patel, Nishant Doshi, Security and Privacy Issues in Cloud, Fog and Edge Computing, Volume 160, Pages 734-739 (2019), ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2019.11.018>.
- [2] G. Cui *et al.*, "Efficient Verification of Edge Data Integrity in Edge Computing Environment," in *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3233-3244, 1 Nov.-Dec. (2022), doi: 10.1109/TSC.2021.3090173.
- [3] Z. Song, H. Ma, R. Zhang, W. Xu and J. Li, "Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2234-2249 (2023), doi: 10.1109/TIFS.2023.3266164.
- [4] B. Jiang, J. Li, H. Wang and H. Song, "Privacy-Preserving Federated Learning for Industrial Edge Computing via Hybrid Differential Privacy and Adaptive Compression," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1136-1144, Feb. (2023), doi: 10.1109/TII.2021.3131175.
- [5] F. Al-Doghman, N. Moustafa, I. Khalil, N. Sohrabi, Z. Tari and A. Y. Zomaya, "AI-Enabled Secure Microservices in Edge Computing: Opportunities and Challenges," in *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1485-1504, 1 March-April (2023), doi: 10.1109/TSC.2022.3155447.
- [6] I. Khan, A. Ghani, S. M. Saqlain, M. U. Ashraf, A. Alzahrani and D. -H. Kim, "Secure Medical Data Against Unauthorized Access Using Decoy Technology in Distributed Edge Computing Networks," in *IEEE Access*, vol. 11, pp. 144560-144573 (2023), doi: 10.1109/ACCESS.2023.3344168.
- [7] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for

- Resource Allocation of Grid Computing,” in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.
- [8] Kumar Sharma, Sandeep & Kumar, Anil & Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems. *Journal of Discrete Mathematical Sciences and Cryptography*. 26. 1415-1425 (2023). 10.47974/JD-MS-1765.
- [9] A. Ahmed, S. Abdullah, S. Iftikhar, I. Ahmad, S. Ajmal and Q. Hus-sain, “A Novel Blockchain Based Secured and QoS Aware IoT Vehicu-lar Network in Edge Cloud Computing,” in *IEEE Access*, vol. 10, pp. 77707-77722 (2022), doi: 10.1109/ACCESS.2022.3192111.
- [10] S. K. Sharma, V. S. Sharma, S. Basheer, A. Chaurasia and C. L. Chowdhary, “An Astute Automaton Model for Objects Extraction Using Outer Totality Cellular Automata (OTCA),” in *IEEE Access*, vol. 11, pp. 123876-123890 (2023), doi: 10.1109/ACCESS.2023.3329473.
- [11] M. Kim *et al.*, “A Secure Batch Authentication Scheme for Multiaccess Edge Computing in 5G-Enabled Intelligent Transportation System,” in *IEEE Access*, vol. 10, pp. 96224-96238 (2022), doi: 10.1109/AC-CESS.2022.3205001.
- [12] Miguel Landry Foko Sindjoun, Mthulisi Velempini, Clémentin Tay-ou Djamegni, “A data security and privacy scheme for user quality of experience in a Mobile Edge Computing-based network, Array”, Vol-ume 19, 100304 (2023), ISSN 2590-0056, <https://doi.org/10.1016/j.array.2023.100304>.
- [13] Alwakeel, A.M. An Overview of Fog Computing and Edge Comput-ing Security and Privacy Issues. *Sensors*, 21, 8226 (2021). <https://doi.org/10.3390/s21248226>.
- [14] Sharma, Sandeep Kumar, C. S. Lamba, and V. S. Rathore. “OTCA Approach Towards Blurred Image Feature Estimation and Enrichment.” *Information and Communication Technology* : 329 (2018).
- [15] Sharma, Sandeep Kumar, C. S. Lamba, and V. S. Rathore. “Ra-dius based cellular automata approach for image processing applications.”IEEE Computer Society (2017).
- [16] Sharma, Sandeep & Lamba, C. & Rathore, Vijay Singh. Incessant Ridge Estimation Using RBCA Model: Proceedings of ICETEAS 2018 (2019). 10.1007/978-981-13-2285-3_25.