Selection based Approach for One-Time Pad Encryption using Checksum and Cellular Automata

G. Kumaresan, N. P. Gopalan

Abstract*: Cloud computing is a technological advantage of information enabled services. Due to the lack of protection and reliability are the main tasks in a public cloud and the present authentication method do not provide adequate security in public cloud. Hence, this paper attempts to propose a three-level selection based One-Time Pad (OTP) encryption method using hybrid cellular automata for the public cloud which satisfies avalanche diffusion and confusion properties. It is found that by combining hybrid cellular automata and checksum method, a robust master key in the public cloud could be generated. The simulation results show that the proposed method has large key space and protects brute force and chosen plaintext attacks in addition to better accessing time for cloud data. The numerical analysis confirmed that the proposed hybrid cellular automata based one-time pad encryption solution provides better security.

***Index Terms*: One-Time Pad, Cellular Automata, Block Encryption, User Security.**

I. INTRODUCTION

The term cloud is a type of computing that runtime accessible, virtualized and the assets are delivered as a service over the internet. It can be accessed anyplace, anytime and anywhere in the planet across the web. As per the National Institute of Standards and Technology [1] explanation, “cloud computing is a method for enabling suitable, ubiquitous, instant network access to collective computing resources that can be quickly supported and released through service provider interaction or minimal management effort”. Cloud computing have three main services: Platform as a Service, Infrastructure as a Service and Software as a Service and its claim can be executed with four operation methods: private cloud, community cloud, hybrid cloud and public cloud [2]-[5]. Also, it includes service level agreements, scalability, pay-per-use, data storage, and prevention methods. Cloud Service Provider (CSP) takes the obligation to provide high security for authenticated user’s secret data anywhere in the world [6] as shown in Fig. 1. Currently, cryptographic block encryption acts a important role in a distributed environment (i.e. public cloud). Generally, the encryption method is used to protect the authenticated user’s secret messages across the web.

Revised Manuscript Received on June 14, 2019.

G. Kumaresan, Research Scholar, Department of Computer Applications, National Institute of Technology, Tiruchirappalli-620015, India.

N. P. Gopalan, Professor, Department of Computer Applications, National Institute of Technology, Tiruchirappalli-620015, India.

Conventional encryption methods do not give sufficient security in public cloud [7]-[10]. Hence, there is a need for capable encryption method in public cloud. As stated in the Kerckhoff’s [11] principle `secrecy of the key alone gives protection. However, the security system is more complicated'. Hereafter, Shannon was transformed [12] as `enemy knows the system'. A lot of researchers presented different techniques and innovative approaches for key generation in public cloud. Still, the cryptographic key generation methods are vulnerable to many attacks in a distributed environment. There is a need for secret keys to strengthening in a public cloud. Hence this paper attempts to strengthen secret keys using hybrid cellular automata.

Fig. 1. Model for Cloud Computing

A. Cellular Automata

A cellular automaton is a discrete dynamical system which is having regular grid of cells. These cells can change their states based on their neighbor's states [13]. Encryption is all about, if the CA global map is returnable, it is possible to retrieves the original cells (i.e. Rule 15 is inverse of Rule 85). The proposed method uses one-time pad (OTP) encryption which is providing total privacy while executing the CA structures during runtime [14]. However, the OTP encryption is need for randomness of the secret key [26]. Hence, the proposed method uses a hybrid cellular automaton which is having best randomness and also without knowing corresponding transition rule the adversary cannot obtain the secret key information as CA has undecidability in nature. The boolean expression of every CA rule illustrated in Table 1.

Table 1: Boolean expression of Hybrid CA rules

S_n	HCA Rule	Boolean Expressions
1	Rule30	$H_i^{t+1} = H_{i-1}^t \oplus [H_i^t \text{ or } H_{i+1}^t]$
2	Rule90	$H_i^{t+1} = H_{i-1}^t \oplus H_{i+1}^t$
3	Rule150	$H_i^{t+1} = H_{i-1}^t \oplus H_i^t \oplus H_{i+1}^t$
4	Rule 165	$H_i^{t+1} = H_{i-1}^t \overline{\oplus} H_{i+1}^t$

II. LITERATURE SURVEY

Digital data protection is one of the immense threats in modern computational systems particularly in public cloud environment. Due to the directness of the public cloud, the adversary carrying lots of attacks. Hence, the previous arts are studied and found the different types of threats. Lots of data security researchers had presented innovative techniques in the public cloud. In [15], proposed an innovative approach for information stored in the open clouds. In their approach, without knowing the user identity, the system evaluates authentication in the cloud. Hence, only genuine users can decrypt the original data. In their system protects replay attacks in the cloud.

Though, the cloud service provider realizes each and every record policy which is stored in the distributed environment. To improve performance, in [16] proposed a multi factor user authentication across a dynamic cloud environment. In their system, the smart phone to acts as unique and only characteristics requires to entrée the services. This method protects denial of service attack and password guessing attack. However, the computational complexity and performance cost are massive to implement the large applications in the distributed environment (i.e., public cloud). Later, in [17] the author use the first factor as username, the second factor as a password with an ATM pin called as M-pin.

It protects brute force attack and replay attack. However, it is unsuccessful for the multi-cloud environment. In [18] proposed a two level authentication model in educational cloud. The data accessing time is very less in comparison with the previous methods. However, the system is an ineffective in the distributed applications. Hereafter, [19] conquer these drawbacks and presented a new approach for authentication. The data stored in the different cloud and it protects brute force attack as key space is enough in their system. However, the computational complexity and running time are large in a multi-cloud environment. Liu *et al.* to decrease the computational performance and designed an innovative model in the public cloud [20].

Authors have used two-factor (i.e., secret key and device). In this system, the cloud server knows the user fulfill data as no idea on the accurate characterization of the user. It prevents possible attacks; however, communication cost and running time are large in the system. To conquer these drawbacks, in [21] proposed a three level authentication model and it reduces an accessing time and prevents a replay attack. In [22] a multi factor verification based data backup model is proposed. This system used symmetrical keys (i.e. same keys are used both encryption and decryption) and is split into two stages then destroy the keys.

This key can be retrieved using smart card and it protects denial of service attack. Later, lots of cellular automata based user authentication methods have been proposed and analyzed in distributed environment [23]-[25] especially in public cloud. However, most of the techniques uses multi-factor authentication and it took more time and also the computational complexity is large in many applications which is vulnerable to chosen plaintext attack and brute force attack. The proposed cellular automata based OTP encryption scheme to overcome these defects.

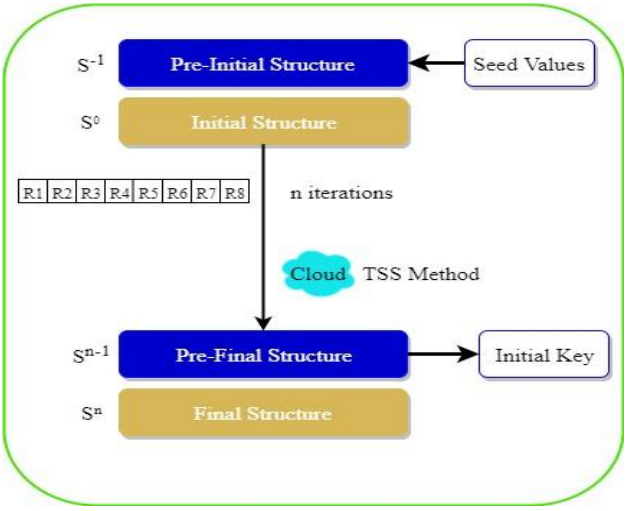

Fig. 2. Process of Key Generation

III. PROPOSED WORK

The main aim of the proposed method is to emphasize user security in distributed environment especially in public cloud. It involves two phases such as registration level and authentication level.

A. Registration Part

The new user's needs to register themselves using digital devices like a laptop, personal computer, smart phone and tablet. After successful registration, the required messages will be sent to the registered users through email and mobile phone.

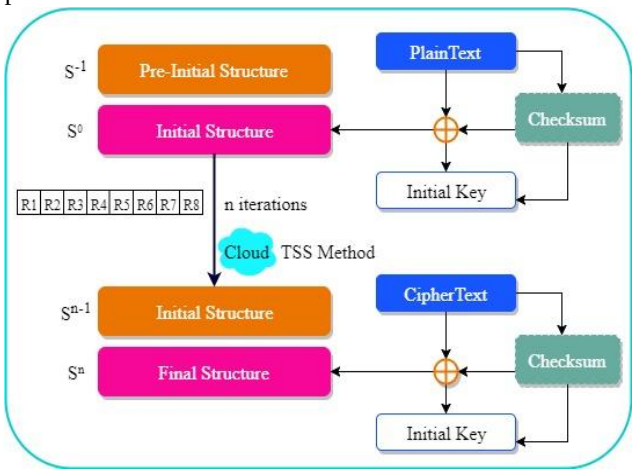

Fig. 3. Process of Encryption

B. Authentication Part

The registered users only can access the authentication page services. Subsequently, hybrid cellular automata based selection process (Three-Level) is proposed to emphasize the user security in public cloud. It begins with four best HCA rules [27] are saved randomly in 2^3 rule vector matrix.

1) User Level Selection

In the proposed method, the first level is done by the registered user who is choosing HCA rule from rule vector matrix which is stored in the memory buffer.

2) CSP Machine Level Selection

Similarly in the second level, the CSP machine randomly choosing a HCA rule from rule vector matrix. Here first iteration result input of the second selection rule.

3) CSP Level Selection

In the third level, the CSP randomly choosing a HCA rule from rule vector matrix. Here second iteration result input of the third selection rule. After iterating 2^{128} times, it produces the output structure.

C. Mode of Operation

In case the authenticated user to enter their credentials into the cloud service access page. The following modes of operations are executed in the proposed system. Initially the logistic function to generate seed value and stored in the pre-initial structure. After 2^{128} iterations (i.e. the rules are selected using TSS method) and it produces the output structure as initial key which is shown in Fig. 2.

The generated initial key XORed with plaintext (i.e. password) and is addition to checksum values as secret key shown in Fig. 3. The key will be send to the authenticated users to acknowledge the same using checksum computations.

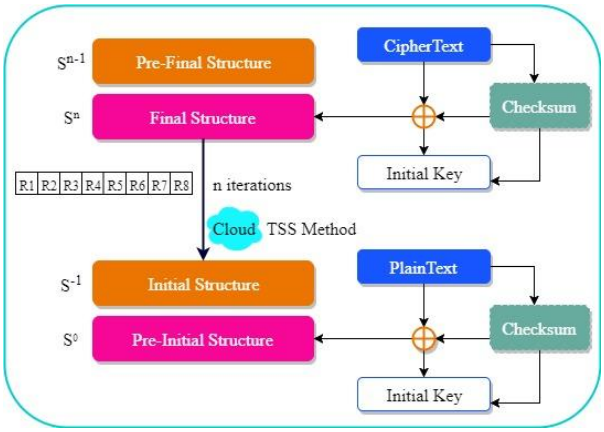

Fig. 4. Process of Decryption

At the end, the authenticated users enter their secret key (i.e. one-time pad) to access the cloud services. The decryption process is done in backward direction shown in Figure 4. In comparison with earlier methods, the proposed method achieves better user security and improves execution time to access the cloud services. The detailed numerical analysis explained in the following section.

IV. NUMERICAL ANALYSIS

A. Correctness of Proposed Key Generation

Let the logistic function [28]

$$x_{n+1} = \mu \times x_n (1 - x_n) \quad (1)$$

be the key seed value for the proposed methodology with the interval from $0 < x_n < 1$ and $3.99 < \mu < 4$. Here μ represents the growth rate and x_n is a population at time n.

Hence proposed method obtained the following matrix:

$$\mathbf{K}_{S\times S} = \begin{bmatrix} 0.145 & 0.321 & 0.551 & 0.613 \\ 0.781 & 0.215 & 0.818 & 0.313 \\ 0.919 & 0.222 & 0.415 & 0.666 \\ 0.585 & 0.414 & 0.323 & 0.718 \end{bmatrix}$$

Hence, every value in the matrix multiplies with 255.

$$\mathbf{K}_{S\times S} = \begin{bmatrix} 0.145 & 0.321 & 0.551 & 0.613 \\ 0.781 & 0.215 & 0.818 & 0.313 \\ 0.919 & 0.222 & 0.415 & 0.666 \\ 0.585 & 0.414 & 0.323 & 0.718 \end{bmatrix} \times 255$$

$$\mathbf{K}_{S\times S} = \begin{bmatrix} 37 & 82 & 141 & 156 \\ 199 & 55 & 209 & 80 \\ 234 & 57 & 106 & 170 \\ 149 & 106 & 82 & 183 \end{bmatrix}$$

The obtained square matrix converted into binary value and is applied into 2's complement method:

$$\mathbf{K}_{S\times S} = \begin{bmatrix} 00100101 & 01010010 & 10001101 & 10011100 \\ 11000111 & 00110111 & 11010001 & 01010000 \\ 11101010 & 00111001 & 01101010 & 10101010 \\ 10010101 & 01101010 & 01010010 & \mathbf{10110111} \end{bmatrix}$$

Hence, the proposed method takes last binary values of the matrix as input for the cellular automata structure. Therefore,

CA1=10110111

According to the following equation, the proposed method uses to select the CA rules in the vector matrix.

$$C = | x_n \times 7 | + 1$$

where x_n is obtained from logistic function from Eq. (1).

First Selection: In case the user select rule 90 (Table 1) from rule vector matrix, the proposed method obtained the following operations:

1 0 1 1 0 1 1 1
↓↓↓↓↓↓↓↓
1 0 1 1 0 10 0

CA1'= 10110100

where CA1' represents first selection first iteration result.

1 0 1 1 0 1 0 0
↓↓↓↓↓↓↓↓
0 0 1 1 0 0 11

CA1''= 00110011

where CA1" represents first selection second iteration result.

Second Selection: Similarly the CSP machine select rule 150 (Table 1) from rule vector matrix the following operations are obtained:

CA2=00110011

0 0 1 1 0 0 1 1
↓↓↓↓↓↓↓↓
1 1 0 0 1 1 0 0

CA2'= 11001100

where CA2' represents second selection first iteration result.

1 1 0 0 1 1 0 0
↓↓↓↓↓↓↓↓
0 0 1 1 0 0 11

CA2''= 00110011

where CA2" represents second selection second iteration result.

Third Selection: CSP select rule 30 (Table 1) from rule vector matrix the following operations are obtained:

CA3=00110011

0 0 1 1 0 0 1 1
↓↓↓↓↓↓↓↓
1 0 1 0 1 01 0

CA3'= 10101010

where CA3' indicates 3rd selection 1st iteration result.

1 0 1 0 1 0 1 0
↓↓↓↓↓↓↓↓
1 1 1 1 1 1 1 1

CA3''= 11111111

where CA3" represents third selection second iteration result.

B. Correctness of Proposed OTP Encryption

Let us consider f is the function of cellular automata structure:

$$f : \{0,1\}^{256} \times \{0,1\}^{256} \rightarrow \{0,1\}^{256} \times \{0,1\}^{256}$$
$$(\mathrm{M}_s, \mathrm{I}_k) \rightarrow f(\mathrm{M}_s, \mathrm{I}_k)$$
$$f_t = f(\mathrm{M}_s, \mathrm{I}_k)$$

(E.g.),

Suppose the user Plaintext: 11101001;

Initial key I_k : 11111111 which is obtained by one-time pad key K_{otp}

$$\mathrm{I}_k = 11111111$$
$$\mathrm{K}_{otp} = 11101001 \oplus 11111111$$
$$\mathrm{K}_{otp} = 00010110$$

Add checksum into OTP key K_{otp}. Hence, the proposed method computes the parity value:

$$\mathrm{K}_{otp} = 0+0+0+1+0+1+1+0 (\mathrm{mod}\ 2) = 1$$

Then the proposed method adds an odd parity bit $\boxed{1}$ into K_{otp} .and send to destination side.

$$\mathrm{K}_{otp} = 00010110\boxed{1}$$

C. Correctness of Proposed Decryption

After receiving key K_{otp} (i.e. 22) with parity bit $\boxed{1}$, the user calculates and ensures the correct transmission in the destination.

$$\mathrm{K}_{otp} = 00010110 + \boxed{1}$$
$$\mathrm{K}_{otp} = 0+0+0+1+0+1+1+0+1 (\mathrm{mod}\ 2) = 0$$

The proposed method

acknowledges correct transmission after observing expected even result (i.e., odd parity bit method). After that, the authenticated user to enter the correct code and obtained the following mode of operations.

$$f_1 : \{0,1\}^{256} \times \{0,1\}^{256} \rightarrow \{0,1\}^{256} \times \{0,1\}^{256}$$

$$(\mathrm{I}_k, \mathrm{M}_s) \rightarrow f_1(\mathrm{I}_k, \mathrm{M}_s)$$

$$\mathrm{K}_{otp} = \mathrm{K}_{otp}(\mathrm{I}_k, \mathrm{M}_s)$$

The decryption process is done in similar way. The proposed method noted that the similar CA rules are applied while it encrypting the initial structure. Hence the proposed method obtains the plaintext and initial key.

Plaintext: 11101001

Initial Key: 11111111

D. Avalanche, Confusion and Diffusion properties

As stated in Kerckhoffs's principle, the master key should satisfy avalanche criterion, confusion and diffusion properties. Avalanche criterion is all about when an input changes a small and the outcome varies extremely. In case the small varies in the master key or plaintext should origin the extremely vary in the ciphertext. The proposed method achieves avalanche criterion by using logistic function and hybrid cellular automata rules. Diffusion property all about, the correlation between plaintext and ciphertext should be complicated as much as possible. The proposed method achieves this property using hybrid CA rules. Confusion property is all about, the correlation between master key and ciphertext should be complicated as much as possible. The proposed method achieves this property using hybrid CA mechanism and it makes the complex behavior. Therefore, the proposed method assuages the basic three properties and it prevents chosen plaintext attack.

E. Key space analysis

Different keys are generated based on the user's requirements. Hence, the authenticated user's plaintext and initial key are combined, then iterated and it produces the master key. Every key situate 128-bit key length and the total key size is 2^{128} and is enough to protect brute force attack. The CA holds 256-bit for each block and is used for encryption and decryption which is having $2^{8X\,256X\,256}$ space size. Hence, the key space is sufficient to protect all possible attacks.

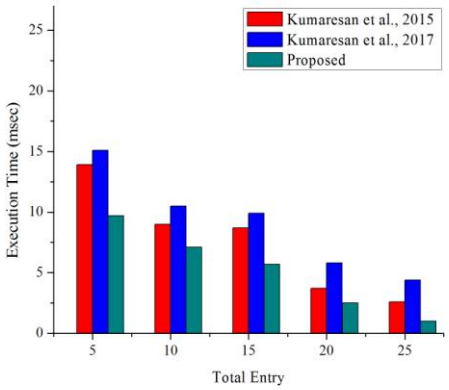

Fig. 5. Comparison of Execution Time

V.EXPERIMENTAL RESULTS

In our experiment, the designed model has been verified in the virtual public cloud. Depend on CSP total entry the execution times are calculated using Eq. 2. Hence, the proposed method obtained good results in comparison with existing methods that are shown in Fig. 5.

Also, the proposed method achieved better improvement speed in comparison with previous methods that are shown in Table 2.

$$\text{Speed}(\%) = \frac{\delta - \eta}{\delta} \times 100 \qquad (2)$$

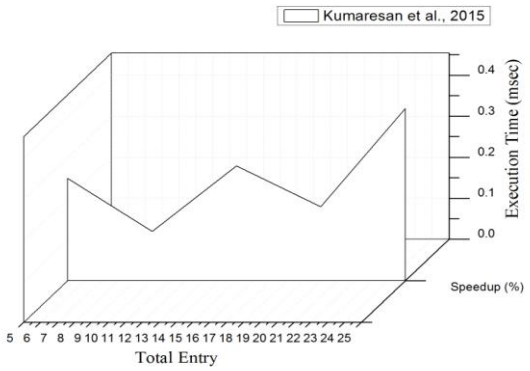

Fig. 6. Kumaresan *et al.*, 2015 improvement

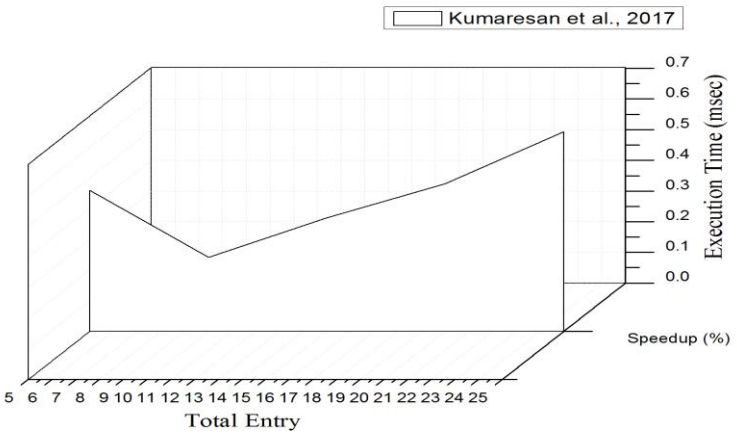

Fig. 7. Kumaresan *et al.*, 2017 improvement

Table 2. Illustration of Execution Time (msec)

Entry	(Kumaresan et al., 2015)	(Kumaresan et al., 2017)	Proposed	Speed	Speed
19	13.9	15.1	10.3	0.25	0.46
14	9.0	10.5	7.9	0.12	0.24
10	8.7	9.9	6.2	0.28	0.37
6	3.7	5.8	3.0	0.18	0.48
2	2.6	4.4	1.5	0.42	0.65

where δ represents existing factor and η represents proposed factor. It has been noticed that based on the number of entries there is an improvement in speed that is shown in Fig. 6 and Fig. 7. It is noted that, number of entries increased the improvement speed is decreased and so on.

VI. CONCLUSION

Hybrid cellular automata based one-time pad encryption method has been proposed and analyzed in the virtual public cloud. The proposed method generated key protects brute force and chosen plaintext attacks and it satisfied avalanche, diffusion and confusion properties. Also, in comparison with earlier methods, proposed method provides enhanced security and improves accessing time for cloud data.

REFERENCES

1. Mell. P, Grance. T, "The NIST definition of cloud computing version 15 technical report", *Computer and information Sciences*, 53(6), 2009, pp.1-10.
2. Vaquero. L, Rodero-Merino. L, Caceres. J, and Lindner. M, "A break in the clouds toward a cloud definition", *ACM sigcomm computer communication review*, 39, 2009, pp.50-55.
3. Badger. L, Bohn. R, Chu. S, Hogan. M, Liu. F, Viktor Kaufmann and Jian, "*Useful information for cloud adopters", NIST cloud computing program*, 2(1), 2011, pp.1-73.
4. Buyya. R, Yeo. C and Vengopal. S, "Market oriented cloud computing vision, hype, and reality for delivering IT services as computing utilities*", proceedings of the 10th IEEE international conference on high performance computing and communications*, 2008, pp.5-13.
5. Buyya. R, Yeo. C, Venugopal. S, Broberg. J, and Brandic. I, "Cloud computing and emerging IT platforms vision hype and reality for delivering computing as the 5th utility", *Further generation computer systems*, 25, 2009, pp.599-616.
6. Subashini. S, Kavitha. V, "A survery on security issues in service delivery models of cloud computing", *Journal of network and computer applications*, 2011, pp.1-11.
7. Viega. L, "Cloud computing and common man", *Computer*, 42(8), 2009, pp.106-08.
8. Wang. C, et al., "Ensuring data storage security in cloud computing", *Proceedings of the 2009 17th International Workshop on Quality of Service (IEEE)*, 2009, pp.1-9.
9. Michael. E. et al., "In defense of the realm: Understanding the threats to information security", *International Journal of Information Management*, 24, 2004, pp.43-57.
10. Zissis. D , Lekkas. D, "Addressing cloud com-putting security issues", *Future Generation Computer Systems*, 28, 2012, pp.583-592.
11. Kerckhoff's. A, "La cryptographie militaire,"*Journal des sciences militaires*, 1883, volume 9, pp. 161-191.
12. Shannon. C, "Communication theory of secrecy systems,"*Bell System Technical Journal*, 1949.
13. Kumaresan. G, Gopalan. N. P, "An analytical study of cellular automata and its applications in cryptography," *International journal of computer network and information security*, 2017, volume 9, no.12, pp.45-54.

14. Anghelescu. P, "Encryption algorithm using programmable cellular automata,"*IEEE World Congress on Internet Securiyt*, 2011, pp. 233-239.
15. Ruj. S, Stojmenovic. M and Nayak. A, "Decentralized access control with anonymous authentication of data stored in clouds", IEEE Transactions on Parallel and Distributed Systems, 25, 2014, pp. 384-394.
16. Z. Siddiqui, A. Abdullah and A. Alghamdi, "Smart environment as a service: Three factor cloud based user authentication for telecare medical information system", *Journal of Medical Systems*, 38, 2014, pp. 9997.
17. Nitin. N and Ugrasen. S, "Two factor authentication using M-pin server for secure cloud computing environment", International Journal of Cloud Applications and Computing, 4, 2014, pp. 42-54.
18. Kumaresan. G, Veeraragavan. N and Arockiam. L, "A dynamic two stage authentication framework to enhance security in public educloud," *International journal of applied engineering research*, 2015, volume 10, no. 82, pp. 126-131.
19. Song. S, Lee. J and Jun. M, "User authentication method design based on biometrics in a multi-cloud environment", *Journal of Advances in Computer Science and Ubiquitous Computing*, 373, pp. 283-288.
20. Liu. J. K, Au. K and Li. J, "Fine grained two factor access control for web based cloud computing services", *IEEE Transactions on Information Forensics and Security*, 11, 2016, pp. 484-197.
21. Kumaresan. G, Gopalan. N. P, "EduCloud: A dynamic three stage authentication framework to enhance security in public cloud," *International journal of engineering and manufacturing*, 2017, volume 7, no.6, pp.12-26.
22. Liu. Y, Zhong. Q and Cheng. C, "A secure data backup scheme using multi-factor authentication", *Journal of Information Security*, 11, 2017, pp. 250-255.
23. Chai. Z, Cao. Z and Zhou. Y, "Encryption based on reversible second order cellular automata,"*Springer Conference on Parallel and Distributed Processing and Applications*, Berlin, 2005 volume 3759.
24. Zhang. X, Zhang, H and Xu. C, "A reverse iteration encryption scheme using layered cellular automata", International Conferece on Information and Communication Technologies, 2015, pp. 1-7.
25. Czerniak, J. M. Zarzycki, H. A. L. P.W. and Kardasz. P, "A cellular automata –based simulation tool for real fire accident prevention", *Mathematical Problems in Engineering*, 2018, pp. 1-12.
26. Stallings. W, "Cryptography and network security: principles and practice" *Prentice Hall*, 2011.
27. Tomassini. M and Perrenoud. M, "Stream ciphers with one and two-dimensional cellular automata, in: 341 m. schoenauer et al. (eds.)", Parraallel Problem Solving from Nature, 342, 2000, 722-731.
28. Wu. G and Baleanu. D, "Discrete fractional logistic map and its chaos", *Nonlinear Dynamics*, 75, pp. 283-287.

AUTHORS' PROFILES

G. Kumaresan: Research Scholar at Department of Computer Applications, National Institute of Technology Tiruchirappalli. He received MCA from Thiagarajar College of Engineering, Madurai, India. M.Tech from Bharathidasan University, Tiruchirappalli, India and M.Phil. from St.Joseph College, Tiruchirappalli, India. He has four years experience in teaching as an Assistant Professor. His areas of interest include Cellular Automata based Cryptography and Cloud Security.

N. P. Gopalan: is Professor of Computer Applications Department at National Institute of Technology, Tiruchirappalli, Tamil Nadu, and India. He obtained his PhD from the Indian Institute of Science, Bangalore. His research interests lie in Data Mining, Cryptography, Distributed Computing and Theoretical Computer Science.