IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
Research Paper © 2012 IJFANS. All Rights Reserved UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

A ENHANCED LOGISTIC CHOATIC ENCRYPTION ALGORITHM FOR ENSURING THE SECURED DATA TRANSMISSION TO COUNERFEIT THE ATTACKS.

[1]J.Praveen Kumar, [2]M.Suresh Babu

[1]Research Scholars in Department of Computer Science Bhartiar University Coimbatore.

[2]Professor in Department of CSE, Teegala Krishna Reddy Engineering College Hyderabad

[1]praveentkrecit@gmail.com, [2]sureshcse@tkrec.ac.in

Abstract

Cloud computing is meant for storing the huge data using third party that ensures that confidential data cannot be accessed by the other users. But with rapid growth of technologies, data in the cloud normally increases which questions its security in storing in the cloud. Hence the protecting the cloud data seeks the strong security levels to counterfeit the different cloud attack. This study suggests the strong encryption algorithm accompanied by the hybrid combination of the chaotic scroll and logistic maps to establish the high end security to the cloud data. The proposed model exhibits the following advantages over the other algorithms: 1) High dynamic key generation 2) ability to counterfeit the multiple attacks 3) High randomness encrypted data which can provide more confusion of hacking from the intruder's insight. To prove the strength of the proposed model, comprehensive trials are conducted utilizing extensive experimentation of the NIST (National Institute of Science and technology) in which different statistical tests experiments were conducted to validate the robustness of the suggested model. Additionally, The Burrows-Abadi-Needham Logic (BAN) serves as a formal assessment mechanism to evaluate and scrutinize the suggested methodology's security phase. Both the Profverif tool and AVISPA are employed for comprehensive validation of the given model. Also the randomness of the suggested model is assessed with the other residing algorithm in means of communication cost and randomness. Results demonstrates that the proposed model shows its ability to provide more potent protection to the cloud data than the other existing encryption algorithms.

Keywords: Cloud Computing, Security, Chaotic Encryption, Scroll and Logistic maps, NIST, Burroes-Abadi-Needham, AVISPA.

Section-1

Introduction :

The cloud serves as an accessible and communal platform for storing data from the Internet of things (IoT) devices. It provides an users to access the data with a comprehensive online service offering available at all times and from any location, users can access a multitude of options. However, growth of intruders in attacking the data normally grows exponentially, which affects the protection of information housed within cloud infrastructure. Hence

ensuring the security in cloud data has become the high priority research in the perspective of user data protection.

Numerous established methodologies prioritize safeguarding data privacy, ciphertext-driven data retrieval, and proof of possession via ciphertext. However, the security of cloud systems and devices remains susceptible to compromise through the exploitation of vulnerabilities such as fraud, espionage, and falsification, perpetrated by either persistent external adversaries or malevolent internal entities [1-2]. Despite the robust defensive algorithms exhibited by existing strategies [3], the integrity of cloud environments and gadgets remains at risk.

As a result, to address the situation described above, customization of encryption techniques is imperative in a cloud setting. The ongoing investigation endeavors to develop a robust encryption algorithm utilizing chaos theory and symmetric key cryptography to address the demand for data security. Nevertheless, the methods proposed by existing encryption protocols in the mentioned scenario result in considerable operational costs. However, the approaches outlined by the existing encryption algorithms needs more space, non-susceptible to attacks and high chance of the data inprotection. In response to this deficiency, this research proposes the strong chaotic encryption with hybrid combination of the scroll and T logistic mapping approach is advocated as the optimal strategy for ensuring maximum security of clinically sensitive data. This proposed model encapsulates the key findings of the research study, offering a novel solution to safeguarding confidential information in a clinical context.

1. Proposes the logistic Chaotic Encryption Scheme to counterfeit the multiple attacks and to provide high secured protection to the data.
2. Utilize the code for the devised system within the renowned AVISPA tool [4] and the ProVerif program [5] to authenticate the correctness of the informal security assessment.
3. Utilize the NIST standards for assessing and contrasting with existing schemes to exhibit the superiority of the suggested scheme in means of supremacy and resilience against both active and passive attacks [6]. Additionally, it effectively fulfils the goal of ensuring heightened privacy.

The subsequent sections of this paper are organized as follows: Section 2 delves into diverse encryption methodologies proposed by different scholars. In Section IV, a comprehensive elucidation of key generation and encryption procedures is provided, alongside discussions on multi-scroll and logistic maps. Section VI presents an empirical validation of the security analysis, coupled with a comparative examination. Lastly, Section V encapsulates the paper's conclusions concerning prospective enhancements.

Section-2

Related Works:

Efficient Probabilistic Public Key Encryption (EPPKE), a technique proposed by M.G. Aruna et al. in 2020, is enhanced using Covariance Matrix Adaptation Evolution Strategies (CMA-ES). The Luhn method with BLAKE 2B encapsulation is used to guarantee

data integrity. For data that has been moved to the cloud, this increases security. In the end, the encryption and decryption times of 0.61 and 0.5 seconds, respectively, showed the system's outstanding security and speed. The primary drawback of this system, however, is that it uses more energy when there is a lot of network traffic [7].

A hybrid cloud security Attribute-Based Encryption approach with Support for Dynamic Attributes (ABE-DAS) was introduced by P. Kanchanadevi et al. in 2020. Significantly reducing data leakage and protecting data privacy are the goals of this architecture. Dealing with dynamic and mobile location transformation may also be handled using this method. Despite that, this structure's higher communication cost is noted as its primary disadvantage [8].

In their 2022 paper, M. Zeng and colleagues introduced a novel forward-secure method for encrypting data that enables searching using public keys.aimed at preventing cloud servers from accessing any information regarding recently added encrypted data files containing previously queried keywords. Within this framework, they also outlined a method for developing forward-secure public key searchable encryption schemes using attribute-based searchable encryption, thereby aiding users in understanding the underlying design concept. However, the primary drawback of this system, despite its efficacy in ensuring security, lies in its heightened temporal complexity [9].

K. Loganathan et al. (2021) suggested an effective Double-Layer Password Encryption (DLPE) technique to provide a secure credential management system. The creation of unbreakable passwords and preventing password theft by outsiders are essential for safeguarding of passcodes is of utmost importance. The creation of unbreakable passcode and preventing password theft by outsiders are essential to the security of passwords. Dual cryptology reduces the likelihood of finding information defects, malignant assaults, and application hackers, and achieves protected data access without the need of harmful attackers thanks to its strong password capability. Password management was made possible by the integrity and secrecy of the data. This approach, however, is extremely costly to implement in real time [10].

The data safety offered by cloud computing was improved by a method that was introduced by A. Kumar et al. in 2020. Data about users data is secured through the application of RSA and AES encryption techniques in the recommended fix. Better data protection may be achieved prior to cloud storage thanks to the hybridization of these two techniques. To create the Hash Message Authentication Code (HMAC), the assured hash algorithm 512 is employed. Third-party auditors (TPAs) can now utilise a reliable audit package. In the case of heavy network traffic, this architecture also offers great data security. This framework's longer authentication time, however, is a drawback [11].

Efficient Dynamic Searchable Symmetric Encryption (SEDSSE), which was introduced by H. Li et al. in 2020, is a method for protecting cloud-based medical information. Utilizing the protected K-Nearest Neighbour (KNN) and Attribute-Based Encryption (ABE) approaches, this strategy created a dynamically searchable symmetric

Research Paper © 2012 IJFANS. All Rights Reserved

encryption system that will ensure & upholding simultaneous Onward and backward privacy. In addition to improving storage, search, and update difficulty, it overcomes the key sharing issue. Storage overhead, index creation, trapdoor generation, and query speed are all efficiently handled by this architecture. However, this structure's pivotal drawback is, it uses more resources to keep performing at the same level even with high network traffic [12].

Y. Shin et al. (2020) suggested server-aided encryption approaches to achieve maximal secrecy while incurring the expense of operating a key server. The main goal of this plan is to develop an inter-key server duplicate elimination algorithm, which will enable cloud storing platform providers to execute deduplication across ciphertexts from various key servers within or between tenants. The synchronization or advance disclosure of confidential information across Key servers was accomplished by this scheme's decentralised design, which did not depend on any centralised bodies. It enables cloud storing platform to provide superior duplication reduction efficacy and robustness while maintaining high information secrecy. The fundamental flaw with this system, though, is that it takes longer to complete handoff operations in real-time scenarios [13].

A successful Fuzzy Semantic Searchable Encryption strategy (FSSE) was introduced by G. Liu et al. in 2020. This technique allows for multi-term searches securely encrypted data. This framework allows fuzzy search since it is based on the technique for creating fingerprints and Hamming distance. This framework expanded the query keywords and determined how semantically comparable the enlarged word of the query keywords was to the original query keywords in order to accomplish semantic search. This plan is more effective, improves system usability, and provides the security promise of searchable encryption. However, this architecture has a drawback due to its high energy usage [14].

Table 1: Quick overview of residing works

Authors	Methodologies utilized	Merits	Demerits
M. G. Aruna et al., (2020) [15]	EPPKE	High speed encryption	Require more energy
P. Kanchanadevi et al., (2020) [16]	ABE-DAS	Suited for handling dynamic and movable location transformation	High communication overhead
M. Zeng et al., (2022) [17]	Forward secure public key searchable encryption scheme	High efficiency	High time complexity
K. Loganathan et	DLPE	Data integrity, confidentiality	Highly expensive framework for real

al., (2021) [18]		enabled password management	time scenarios
A. Kumar et al., (2020) [19]	RSA algorithm and the AES algorithm	High data protection under dense network traffic	Require more time for authentication
H. Li et al., (2020) [20]	KNN and ABE technique	Efficient performance in terms storage overhead, index building, trapdoor generating and query.	More resource consumption
Y. Shin et al., (2020) [21]	Server-aided encryption schemes	High scalability while preserving strong data confidentiality	Requires more time for handoff operations in real time scenarios
G. Liu et al., (2020) [22]	FSSE	Enhances system usability and more efficient	High energy consumption

Section-3

This section discusses about the logistic maps, scroll maps and proposed encryption schemes

3.1 Logistic Maps – An Overview:

As explored in references [20-22], 3D logistic chaotic maps exhibit greater chaotic properties compared to their 1D counterparts. The mathematical formulations for 3D logistic maps are expressed as follows.

$$X = \mu x\big(1 - x(i)\big) + \beta y' X + \alpha Z \quad (1)$$

$$Y = \mu y\big(1 - y(i)\big) + \beta x' Z + \alpha Y \quad (2)$$

$$Z = \mu z\big(1 - z(i)\big) + \beta z' y + \alpha X \quad (3)$$

When the $\mathbf{0.35} < \mu < 0.381$, $\beta < 0.0022$ and $\alpha = 0.0015$,he given equations demonstrate the 3D Logistic maps. The illustration depicts the phenomenon of Chaos for the specified parameters in the proposed 3D chaotic systems.

Research Paper © 2012 IJFANS. All Rights Reserved

3.3 Key Generation Process:

To generate the high complexity keys, high randomness initial condition are used for the formation of the chaotic equations. After calculating the initial parameters, sophisticated cryptographic keys are generated at the initial stage entails serving as the inputs for the logistic Maps. The diffusion operation is employed by the proposed output to generate the new key which can acts as the high randomness keys. The outputs from the logistic maps acts as the initial conditions to the scroll attractors.

Step 1: As the first step, initial conditions for the logistic maps are calculated and defined for the chaotic outputs

Step 2: Logistic Maps are created based on the initial conditions formed. These are considered as the inputs to the multi-scroll maps.

Step 3: Chaotic maps are formed by the logistic output maps as described in Step 2 .

Step 4: The sensor data from the devices and innovative hybrid Logistic maps undergo diffusion to generate a high-entropy key (Ek) characterized by significant randomness.

$$E_k = D\big(I, LSM(X, Y, Z)\big)$$

$$where\ I = \ Devices\ \ Sensor\ values\ and\ X, Y, Z\ are\ the\ Chaotic\ matrix\ Values$$

Step 5: High randomness Encrypted Data is formed by adopting the diffusion between the key generated and input data.

$$Encrypted\ Data = I * E_k\ scaled\ to\ L$$

$$where\ L\ presents\ the\ Length\ of\ the\ Data$$

Section-4

4.1 Implementation Details :

The complete algorithm was developed using Python 3.10 and implemented on the PC workstation with I7 CPU, 2TB Hard Disk , 16GB RAM and 3.2 GhZ operating frequency.

4.2 Results and Discussion:

4.2.1 Statistical Randomness Analysis:

The integrity of every encryption system's security is paramount is intricately tied to the quality of the key employed in the encryption and decryption processes. In a symmetric encryption setup, where the same key is used for both operations, the vulnerability of a device increases significantly once an adversary gains possession of the key. Thus, it is

Research Paper © 2012 IJFANS. All Rights Reserved

imperative to guarantee that the key generator produces genuinely random keys, thereby thwarting any attempts to breach the system's defences.

Pseudorandom number generation for cryptographic purposes necessitates unpredictability: should initial conditions remain unknown, adversaries should be unable to anticipate the upcoming element in the generated series would be the subsequent bit, regardless of any prior knowledge they possess regarding preceding random numbers. The National Institute of Standards and Technology (NIST) provides a suite of statistical tests for assessing the randomness of number sequences, ensuring their suitability for cryptographic applications. These tests are crucial for identifying any deviations from randomness within a given binary sequence, often attributable to inadequately designed generators. The study employs a range of statistical tests outlined by NIST to demonstrate the attainment of peak variability in the generated keys. Throughout this evaluation, keys produced at each iteration are transformed to binary values using Micro Python libraries embedded within microcontroller boards.

4.2.2 Frequency Monobit Test:

The examination centres around analysing the equilibrium between zeros and ones throughout the complete order. Its objective is to establish if the distribution of ones and zeros corresponds closely to what might anticipate the characteristics of an authentically random sequence. The experiment evaluates the proximity of the proportion of ones to ½, indicating that the quantity of ones and zeros in a sequence should be approximately equal. The success of all subsequent assessments depends on the satisfactory completion of this specific test. In this examination, zeros are designated as -1 and ones are designated as +1, then aggregated to generate cumulative figures, with the overall mathematical expression depicted as below:

$$S = ||S(n)||/n^{0.5} \qquad (4)$$

Once the summation of values, denoted by S(n), is computed here 'n' signifies the entire samples, randomness is assessed through the derivation of a P-value. The mathematical formulation for the P-value is subsequently employed to gauge the randomness.

$$P= \text{erfc}(S/(2)^{0.5} \qquad (5)$$

Table 2 : The parameters derived from the frequency monobit tests are organized in the presented table.

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1			P=0.07583	
2			P=0.045383	
3			P= 0.05342	
4	Frequency		P=0.04359	PASS
5	Monobit	P>0.01	P=0.06702	
6			P=0.090223	
7			P=0.06435	

8	P=0.08945
9	P=0.89334
10	P=0.089345

In each of the ten iterations, keys produced by the CHILS mappings have consistently demonstrated genuine randomness, showcasing their efficacy as robust encryption tools capable of fortifying network defenses against attacks.

4.2.2 Frequency Monobit Test:

The examination concentrates on the ratio of ones present within k-bit segments. The aim to ascertain regardless of the occurrence of ones in a k-bit segment aligns around with k/2, as anticipated on the premise of variability. When the block size k equals 1, this assessment reduces to test 1, the Frequency (Monobit) test. Within this evaluation, K-bit encryption undergoes subdivision into K/2 sections for each cycle, where the randomness is evaluated through a mathematical formula.

$$P = igamc(\frac{N}{2}, \frac{¥^{0.5}(obs)}{2}) \quad (6)$$

Where $igamc$ is the gamma function used for calculation of randomness, $¥ = statistical\ randomess\ value\ which\ is\ given\ by\ the\ mathematical\ expression$

Table 3

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1			P=0.0345	
2			P=.0.33222	
3			P= 0.23450	
4	Frequency		P=0.02345	PASS
5	Block bit	P>0.01	P=0.2893	
6			P=0.19024	
7			P=0.8934	
8			P=0.02345	
9			P=0.08323	
10			P=0.0566	

In every version, the randomness measure exceeds 0.01 for each key generated and scrutinized under two circumstances. The table delineates the mean assessment of the trials conducted within the key segments.

4.3.2 Run Test :

The target of the study is to evaluate the total instances of consecutive identical bits within a series, where a "run" refers to such a sequence. A run, defined by a length denoted as "k," is composed entirely ofk consecutive identical bits, bordered by bits of opposite values on either

Research Paper © 2012 IJFANS. All Rights Reserved

side. The objective of the runs test is to ascertain in regardless of the occurrence frequencies of runs containing ones and zeros of varying extents follow the anticipated distribution for a randomly generated series. Specifically, this test endeavours to discern in regardless of the transition among zeros and ones occurs at a pace either exceeding or lagging expectations.

This examination requires the frequency test as prerequisites, which are conducted in preceding instances. The consistency of the key is scrutinized for its randomness, as depicted in the provided mathematical expression.

$$P = erfc(|V(n)(obs) - 2n\pi(1-\pi)|)/2.828n\pi(1-\pi) \quad (7)$$

Where V(n)(obs)= has to be done

Table 4

No of iteration	Test nature	Decision Rule	Randomness value	Key Test
1			P=0.2290	
2			P=0.3222	
3			P= 0.2894	
4	Run test		P=0.3780	PASS
5		P>0.01	P=0.28920	
6			P=0.22022	
7			P=0.10456	
8			P=0.22303	
9			P=0.3450	
10			P=0.29034	

During the assessment, V(n)(Obs) identified the swift oscillations (characterized as shifts between ones and zeros) occurring when numerous changes occur within the bit sequences. Consequently, the substantial pseudo-randomness is implemented for the bit generation utilizing the suggested logistic chaotic mappings.

4.3.3 Longest Run Test :

The examination focuses on the lengthiest succession of ones within segments of M bits. The objective is to ascertain if the duration of the extended consecutive set of ones in the examined series matches the anticipated in a random sequence. It's important to highlight that any deviation from the expected longest streak of ones also implies a discrepancy in the anticipated length of the prolonged streak of zeros. The selection of M-values adheres to the specifications outlined in the NIST standard, as provided in the accompanying table.

Table 5

Minimum n sequence	Maximum M values
128	8
6272	128
750,000	10^4

ISSN PRINT 2319 1775 Online 2320 7876
Research Paper © 2012 IJFANS. All Rights Reserved UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

4.3.4 DFT Test:

This examination seeks to assess the highest points within the Discrete Fourier Transform of the series, with the main aim being the recognition of cyclic attributes. Its purpose is to identify repetitive trends within the analysed series, which could imply a departure from the presumption of variability. The goal is to ascertain in regardless of the quantity of heights surpassing the 95% boundary considerably deviates from 5%. The mathematical expressions are calculated by the following

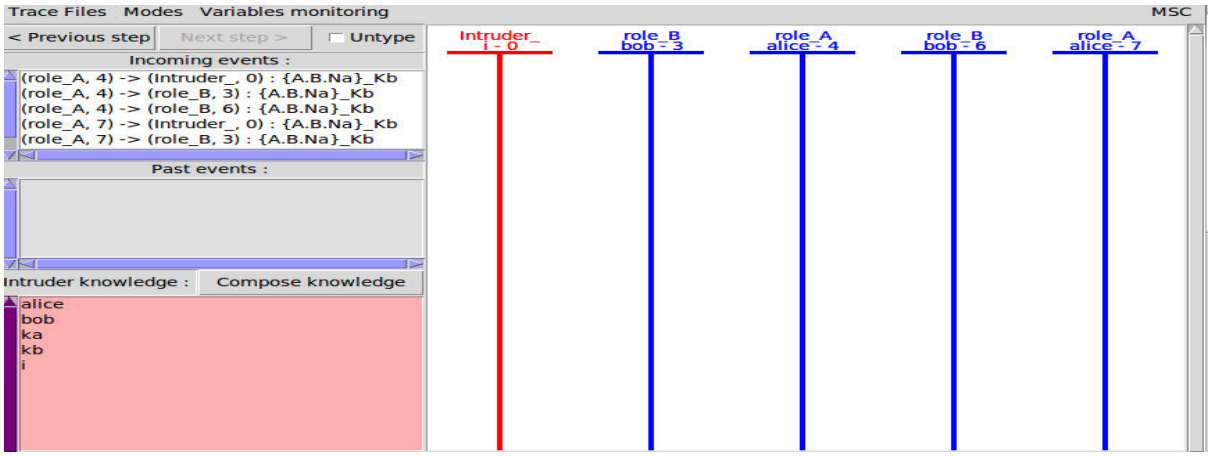
Table 6

Iteration	N	N1	N2	D1	P	Key test(P>0.1)
1	100	44.5	68.5	-1.67	0.457	
2	100	43.4	67.4	-2.45	0.3457	
3	100	44.3	74.6	-3.56	0.3290	
4	100	44	74.5	-2.56	0.8940	
5	100	44	73.5	-3.56	0.124	PASS
6	100	50	67	-4.67	0.9012	
7	100	45	68	-2.70	0.905	
8	100	47	69	-3.902	0.895	
9	100	50	70	-4.672	0.906	
10	100	46	71	-1.090	0.906	

In each iteration, the value of d is minimal, while P exceeds 0.01, indicating that the key demonstrates pronounced pseudo-randomness.

4.4 Verification Process:

Utilizing CAS++ and HLPSL for modelling serves to authenticate the specified protocols via AVISPA validation. The procedures are scrutinized for possible security infringements. Figures 1 to 3 display the outcomes of the simulation for the backend Messaging Servers.



ISSN PRINT 2319 1775 Online 2320 7876
Research Paper **© 2012 IJFANS. All Rights Reserved** UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

Figure 1CAS++ Programs Simulated for Proposed algorithm in AVISPA-SPAN Environment

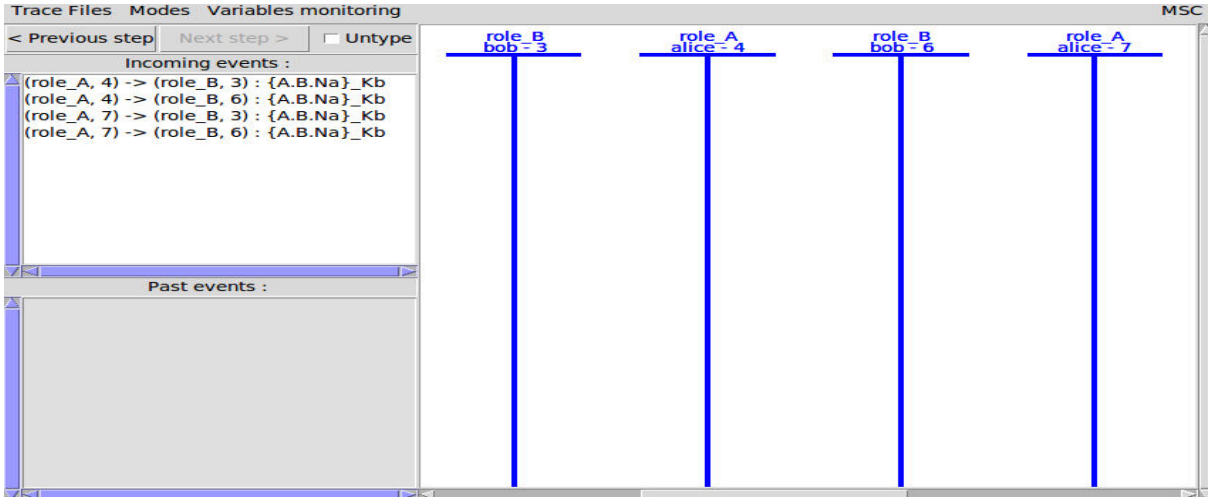


Figure 2Proposed Encryption Process Simulated in AVISPA-SPAN Environment

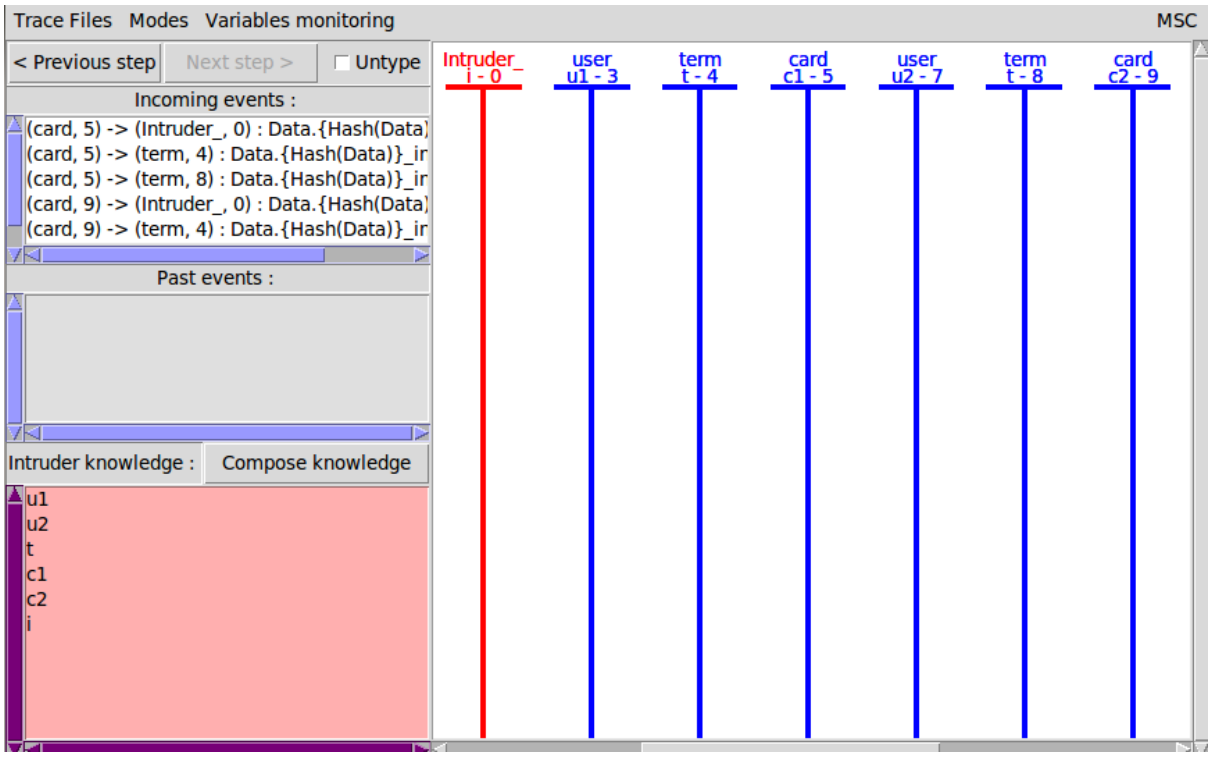


Figure 3 Mutual Authentication Programs (data variables) Simulated in AVISPA-SPAN Environment

Based on simulation results, the proposed protocol effectively repels all attacks and also resolves security concerns within the Cloud setting.

Research Paper © 2012 IJFANS. All Rights Reserved

Section-5

5.1 Conclusion and Future Enhancement:

In this research work, the hybrid scroll logistic maps has been proposed for Cloud data. The proposed work also introduces the permutations and diffusion process which makes the data more random and security. The inclusion of scroll maps and logistic maps are shown the huge change in designing the traditional encryption. Furthermore, strong encryption algorithm system has been designed to evaluate the proposed model whether it is secure from vulnerabilities. The extensive experimentation has been carried and compared with the other existing encryption deployed already for Cloud applications. The results depicts that the suggested methodology is superior than the other residing models without pricing the data security and integrity. Besides, the proposed model passes the NIST statistical tests, that proves its profound diversity behaviour able to repel any assault, this entity possesses unparalleled defence capabilities. Hence the proposed model has a higher level of security with fewer computations and makes its applicable to embed in IoT devices. As the future scope, the proposed S-Box can further be enhanced by the reducing the computations so that it can be deployable in any IoT devices used for smart health care applications.

References:

[1]Ion, M.; Zhang, J.; Schooler, E.M. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-Centric Networking, Hong Kong, China, 12 August 2013; pp. 39–40.

[2] Rahman, Z.; Yi, X.; Khalil, I.; Sumi, M. Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security. In Proceedings of the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Online, 29–30 November 2021; pp. 177–193

[3] Rahaman, Z.; Corraya, A.D.; Sumi, M.A.; Bahar, A.N. A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. arXiv 2020, arXiv:2005.00157. 7. Ziv, J.; Lempel, A. A universal algorithm for sequential data compression. IEEE Trans. Inf. Theory 1977, 23, 337–343.

[4] Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Tamil Nadu, India, 10–11 February 2017; pp. 492–496.

[5] Farooq, U.; Aslam, M.F. Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 295–302.

[6] Kocarev, L. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. 2001, 1, 6–21.

[7] Mukhopadhyay, S.C.; Suryadevara, N.K. Internet of things: Challenges and opportunities. In Internet of Things; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17.

[8] Tausif, M.; Ferzund, J.; Jabbar, S.; Shahzadi, R. Towards designing efficient lightweight ciphers for internet of things. KSII Trans. Internet Inf. Syst. 2017, 11, 4006–4024.

[9] Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A lightweight encryption algorithm for secure internet of things. arXiv 2017, arXiv:1704.08688.

[10] Indrayani, R.; Nugroho, H.A.; Hidayat, R.; Pratama, I. Increasing the security of mp3 steganography using AES Encryption and MD5 hash function. In Proceedings of the 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, Indonesia, 27–28 October 2016; pp. 129–132.

[11] Aljawarneh, S.; Yassein, M.B.; Talafha, W.A. A resource-efficient encryption algorithm for multimedia big data. Multimed. Tools Appl. 2017, 76, 22703–22724

[12] Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley & Sons: Hoboken, NJ, USA, 2007.

[13] M. G. Aruna and K. G. Mohan, "Secured cloud data migration technique by competent probabilistic public key encryption," in China Communications, vol. 17, no. 5, pp. 168-190, May 2020, doi: 10.23919/JCC.2020.05.014.

[14] P. Kanchanadevi, L. Raja, D. Selvapandian and R. Dhanapal, "An Attribute Based Encryption Scheme with Dynamic Attributes Supporting in the Hybrid Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 271-273, doi: 10.1109/I-SMAC49090.2020.9243370.

[15] M. Zeng, H. Qian, J. Chen and K. Zhang, "Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 426-438, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2944367.

[16] K. Loganathan and D. Saranya, "An Extensive Web Security Through Cloud Based Double Layer Password Encryption (DLPE) Algorithm for Secured Management Systems," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526381.

[17] A. Kumar, "A Novel Privacy Preserving HMAC Algorithm Based on Homomorphic Encryption and Auditing for Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 198-202, doi: 10.1109/I-SMAC49090.2020.9243340.

[18] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," in IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 1 April-June 2020, doi: 10.1109/TCC.2017.2769645.

[19] Y. Shin, D. Koo, J. Yun and J. Hur, "Decentralized Server-Aided Encryption for Secure Deduplication in Cloud Storage," in IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1021-1033, 1 Nov.-Dec. 2020, doi: 10.1109/TSC.2017.2748594.

[20] G. Liu, G. Yang, S. Bai, Q. Zhou and H. Dai, "FSSE: An Effective Fuzzy Semantic Searchable Encryption Scheme Over Encrypted Cloud Data," in IEEE Access, vol. 8, pp. 71893-71906, 2020, doi: 10.1109/ACCESS.2020.2966367.

[21] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat and M. U. Ali, "Enhanced Security in Cloud Computing Using Neural Network and Encryption," in IEEE Access, vol. 9, pp. 145785-145799, 2021, doi: 10.1109/ACCESS.2021.3122938.

[22] D. Chen et al., "Privacy-Preserving Encrypted Traffic Inspection With Symmetric Cryptographic Techniques in IoT," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17265-17279, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3155355.