A Novel Technique of Cloud Security Based on Hybrid Encryption by hyper Chaotic Logistic bit scramble

Danish Ahamad[1], Dr.Vijaypal Singh[2]
[1]*PhD Scholar, Department of Computer Science Engineering, OPJS University, Rajasthan, INDIA*
[2]*Associate Professor, Department of Computer Science Engineering, OPJS University, Rajasthan, INDIA*

Abstract- The networks have moved worldwide and information has been considered in the digital form of bits and bytes. Critical information is stored, refined and sent in digital form on personal computers. Since information performs such an essential role, competition are purposing the personal computers for opening up communication programs to either swipe the hypersensitive information or even to agitate the critical information system. There is absolutely no differentiation of cloud aspect or client aspect encryption, so it diminishes the information security. To attain the goals of security system, the encryption algorithms must definitely provide enough power with high security put in place within an Acceptable speed restriction. Therefore, the performance analysis becomes very important to the prevailing encryption algorithms. This paper proposes a novel parallel cryptographic algorithm, Encryption by hyper Chaotic logistic bit Scrambling Encode which can upgrade security.

Keywords- *Cloud computing; Chaotic Scrambling; DNA Encoding*

I. INTRODUCTION

With the Internet accomplishment, there has been a progress in capacity, innovation and preparation, furthermore ending up registering assets being less expensive, more accessible universally and more capable than in any recent memory time. Another registering model is brought forth in acknowledgment by this mechanical pattern basically known as cloud computing which gives assets like CPU and capacity as general utilities that client can discharge and rent on demand through the Internet. The service provider customary part in the cloud computing environment can be isolated in two: rent assets and cloud stages oversee by the infrastructure suppliers based on the estimated model and administration suppliers in which assets are rent from one or more framework suppliers for serving at the client end.

Substantial organizations like Amazon, Microsoft and Google which endeavors giving dependable, more effective and cloud stages that are more cost-proficient and reshaping their business plans undertaken into action by taking advantage through this new worldview. Cloud computing is recognized as the on demand computing considered in which it is internet based processes resources and administer shares computer and other devices on internet. On-appetite computer resources enabling worldwide this model which is organized with shared data pool. The various capability storage solutions are provided to the users and enterprises by the cloud computing such as data storage and processing in third party's data centres. In today scenario, cloud computing is considered to be a progressive area which supplies flexible services dynamically and the software and hardware virtualization over the internet.

Nowadays, cloud computing as a distributing computing is the new growing area in which services are adapted that are dynamically delivered over internet through hardware and software virtualization on demand [1]. As per the users requirement, the cloud computing's biggest advantage is flexibility of the resources release and lease. Moreover, the cloud providers offer the two plan type which is long term and short term reservation plan [2]. The infrastructure in cloud computing is insightful like security, scalability, monitoring and transparency. As an emerging pattern, cloud computing transfers the capabilities of storage to service providers independently. Because the direct control is lost on external data as averse are the users for cloud services acceptance. For building a safer cloud computing system, platforms for services and also considering levels of application software for cloud computing system to be more protected. Encryption of the information is an adequate means in which information security in cloud computing is achieved. Users encrypt the data so as to prevent the unauthorized access by processing or storing the data within cloud based on cryptography. Traditionally, the main point is its focus on information encryption stage that is specified as cloud computing with encrypted data, and system level design implementation. The cloud system based on cryptography allows the data transmission and storage. In the process of information exchange, certification and classification plays a crucial role as assigned with private key and public key or private key only. This way cloud and client develop a relationship. The respective understanding of logical relationship builds the description of data identification, and the dependency of the cloud customer based on the relationship that is logical.

This paper proposes a novel parallel cryptographic algorithm Encryption by hyper Chaotic logistic bit Scramble Encoding which can upgrade security shows in figure 1. First, initial conditions of input text (data) hyper chaotic system are computed and chaotic sequences are generated. Then, bit-level scrambling is implemented to permute the plain text. Section II reviews the literature in context of the cloud security and section III explains the system model and

methodology. Section IV describes the used algorithm and there implementation results are shown in section V. Finally, section VI gives the conclusion and future scope.

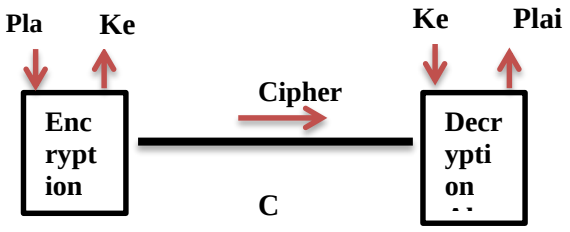


Fig 1: Basic procedure of encryption and decryption

II. LITERATURE REVIEW

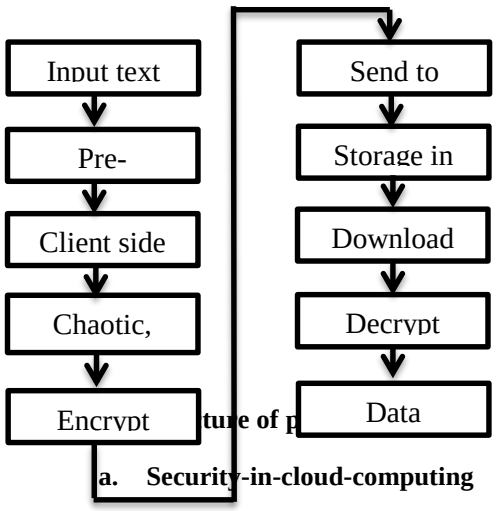
In this paper chaotic systems and RSA encryption algorithm are combined in order to develop an encryption algorithm which accomplishes the modern standards. E.Lorenz's weather forecast' equations which are used to simulate non-linear systems are utilized to create chaotic map. [3] This equation can be used to generate random numbers. In order to achieve up-to-date standards and use online and offline status, a new encryption technique that combines chaotic systems and RSA encryption algorithm has been developed. The combination of RSA algorithm and chaotic systems makes encryption system. [4]In this paper, by using Logistic, Sine and Tent systems we define a combination chaotic system. Some properties of the chaotic system are studied by using figures and numerical results. A color image encryption algorithm is introduced based on new chaotic system. Also this encryption algorithm can be used for binary data. The experimental results of the encryption algorithm show that the encryption algorithm is secure and practical.

Recently, the cryptosystem based on chaos has attracted much attention. Wang and Yu (Commun. Nonlin. Sci. Numer. Simulat. 14 (2009) 574) proposed a block encryptionalgorithm based on dynamic sequences of multiple chaotic systems. We analyze the potential flaws in the algorithm. Then, a chosen-plaintext attack is presented [5]. Some remedial measures are suggested to avoid the flaws effectively. Furthermore, an improved encryption algorithm is proposed to resist the attacks and to keep all the merits of the original cryptosystem.

Analysis on Scrambler Reconstruction with Minimum Priori Knowledge is done using implementation of Scrambler System. The algorithm proposed promises in reconstruction of the LFSR in a synchronous scrambler, as it does not need any initial stage of the input bits, except the source inputs. Location Information Scrambler Architecture for privacy protection on smart phones is presented [6]. They have presented a technique to provide the safety of a user's locale confidentiality based on serviceability, evade the assaulter against revealing any particular POI to the user's ongoing location. A Location information scrambler called a privacy protection system have been designed, implemented and also evaluated by them, which protects the user's location safety by adapting the noise in user's location and therefore, the ambiguity of identifying user's location with any points of interest, while managing resources on mobile devices especially battery energy.

Chaotic sequences can be applied to realize multiple user access and improve the system security for a visible light communication (VLC) system. However, since the map patterns of chaotic sequences are usually well known, eavesdroppers can possibly derive the key parameters of chaotic sequences and subsequently retrieve the information [7]. We design an advanced encryption standard (AES) interleaving aided multiple user access scheme to enhance the security of a chaotic code division multiple access-based visible light communication (C-CDMA-VLC) system. We propose to spread the information with chaotic sequences, and then the spread information is interleaved by an AES algorithm and transmitted over VLC channels [8]. Since the computation complexity of performing inverse operations to deinterleave the information is high, the eavesdroppers in a high speed VLC system cannot retrieve the information in real time; thus, the system security will be enhanced. Moreover, we build a mathematical model for the AES-aided VLC system and derive the theoretical information leakage to analyze the system security. The simulations are performed over VLC channels, and the results demonstrate the effectiveness and high security of our presented AES interleaving aided chaotic CDMA-VLC system and it represented in figure2.

III. PROPOSED ALGORITHM



a. Security-in-cloud-computing

Cloud Computing Security

Cloud computing security refers to the controls that must be implemented in order to prevent the loss of data, information

or resources belonging to a cloud services provider or its customers. Cloud solution providers must implement a variety of security controls for the SaaS (software as a service) solutions, PaaS (platform as a service) solutions and the IaaS (infrastructure as a service) solutions that they provide to their customers or clients.

As with traditional computer or data security, there are many bases that must be covered, in orderto ensure a safe computing environment. Computer security (including cloud computing security)can be implemented by taking the following security measures (as appropriate): restricting access to applications and system resources, logging access & use of applications and systems; and controlling & monitoring access to physical computing resources like servers & data centers, etc.

Many of the security methods that cloud service providers implement are driven by privacy, compliance or legal rules for managing consumer data that specific industries must adhere to. In any event, security breeches can result in major financial losses for any organization, as costly fines and legal expenses may be incurred; along side a loss of confidence in the organization's ability to protect customer data, which can lead to further losses in business revenue.

Public cloud computing security

Since Cloud Computing is an newly evolving model for the delivery of software, platforms and infrastructure; it provides a new set of challenges to IT network and data security personnel [9]. Most organizations that are considering moving their applications to the cloud have a variety of security concerns, which are in many ways, certainly warranted. Ironically, in some cases, a public cloud may provide better security for data and IT resources than what could be provided by a firm's on-premise IT staff; as the element of employee loss or theft of data or computing assets is significantly reduced when an enterprise uses a public cloud services provider to deliver IT services to the organization. Never the less, while public cloud service providers may be able to significantly reduce the threat of employee loss or theft of data or IT assets, they still must competently guard against the outside threat that is intrinsic to delivering services via the Internet: hackers who can launch an attack against the public cloud services being delivered by a cloud service provider.

Private cloud computing security

Private clouds offer the framework for a more secure computing environment than what is available within the sphere of public clouds. Along these lines, many organizations with high security requirements frequently opt to deliver IT services via an enterprise private cloud, which is secured by a network firewall [10]. The implementation of an enterprise private cloud provides organizations with the maximum level of control over their data, applications and systems. An enterprise private cloud eliminates threats from Internet hackers, as well as reducing the occurrence of intellectual property theft, which could easily occur if a company stores its sensitive data and proprietary information in a public cloud. Apprenda's Private PaaS (platform as a service) offering serves as an ideal solution for organizations who want to seamlessly and securely deliver cloud computing services via an enterprise private cloud .

b. Chaotic Theory

All systems can be basically divided into three types:

1. Deterministic systems:

These are systems for which for a given set of conditions the result can be predicted and the output does not vary much with change in initial conditions. Examples are computers.

2. Stochastic/random systems:

These systems,which are not as reliable as deterministic systems. Their output can be predicted only for a certain range of values. Examples are genetic algorithms.

3. Chaotic systems:

These systems are the most unpredictable of the three systems. Moreover they are very sensitive to initial conditions and a small change in initial conditions can bring about a great change in its output. Examples of chaotic systems are the solar system, population growth, stock market, and the weather. Chaos is derived from the Greek word "XĮos", which is meaning a state without predictability or order. A chaotic system is a non-linear, dynamical, and deterministic system which has high sensitive to initial conditions of the system. Chaos system is deterministic system with small change in input results in enormous change in the output, so the system looks as if it is random and prediction becomes impossible (it looks like a noise). It is like butter-fly effect. Due to these properties, chaos theory has been used in cryptography/encryption. In this work, chaotic theory is used for providing security at HW level.

c. Logistic map

Logistic maps are a kind of chaotic system. They have a very simple mathematical form that
gives rise to complex dynamic behavior, and have been widely used in various research fields. The standard equation for a logistic map is:

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

Where $0 < \mu < 4$, $x \in (0, 1)$, $n = 0, 1, 2, \cdots$. When $3.57 < \mu \leq 4$, the map becomes chaotic. To broaden the logistic mapping parameter range and improve its dynamic characteristics, the

logistic map equation has been modified and extended, such as the improved logistic map can be written as:

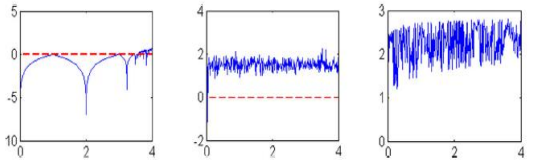
$$x_{n+1} = (L(\mu,x_n)*G(k)) - floor(L(\mu,x_n)*G(k))$$
$$(L(\mu,x_n) = \mu x_n(1-x_n)$$
$$G(K)=2^k, k \in Z, k \geq 8$$

This improved equation exhibits chaotic behavior when $0 < \mu \leq 4$, and the chaotic sequence is more evenly distributed in [0, 14]. However, the iteration of Eq. (3) is still dependent on the initial values of μ and x0. To further enhance the randomness of the chaotic sequences, the logistic map is designed as a segmented function, and the lower four bit-planes of the image to be encrypted are introduced as a control parameter. This improved logistic map is given by:

$$x_{n+1} = (L(\mu,x_n)*G(k)) - floor(L(\mu,x_n)*G(k))$$
$$(L(\mu,x_n) = \mu x_n(1-x_n)$$
$$G(K)=2^k$$
$$K=\begin{cases} j, i <= m \\ j + d(i), < i <= m + lp, j \end{cases} j \in Z, j \geq 8$$

where i is the number of iterations, m denotes the number of terms of the chaotic sequence that are discarded to eliminate the transient effect, d(i) is the element value of the low 4-bit matrix of the data to be encrypted Figure , shows the Lyapunov exponents of the standard logistic map, the improved logistic map , and the proposed logistic map.

The random matrix is used as the control parameter of the proposed logistic map, so that the resulted sequence distribution is more uniform. To evaluate the data distribution of the proposed logistic map, a histogram of chaotic map is constructed. The entire range of



IV. RESULT AND DISCUSSION

In below given tables is comparative analysis of hybrid encryption algorithm. In table, the experiment result encryption file size comparison of Chaotic Logistic bit scramble, Blowfish-MD5 and RSA-MD5 (Rivest, Shamir and Adleman encryption algorithm with message digest hashing algorithm) encryption algorithms are shown. With these hybrid algorithm comparisons, the efficient performance is analysed for cloud environment.

V. CONCLUSION

Although in its early stages of research, the DNA storage is shown to be very effective. The storage of data based on DNA technology is no limited to just science fiction as it is becoming at an increasing rate an important and ubiquitous domain of research by many teams. DNA storage techniques show massive progress. The number of publications related to various DNA based models and techniques increases tenfold annually. Presented methods literally convert each and every smallest possible information into DNA form. Thus 5 this method is highly applicable for handling and storage of massive amounts of various types of data. Although in its early stages of research, the DNA storage is shown to be very effective. The storage of data based on DNA technology is no limited to just science fiction as it is becoming at an increasing rate an important and ubiquitous domain of research by many teams. DNA storage techniques show massive progress. The number of publications related to various DNA based models and techniques increases tenfold annually. Presented methods literally convert each and every smallest possible information into DNA form. Thus 5 this method is highly applicable for handling and storage of massive amounts of various types of data. Although in its early stages of research, the DNA storage is shown to be very effective. The storage of data based on DNA technology is no limited to just science fiction as it is becoming at an increasing rate an important and ubiquitous domain of research by many teams. DNA storage techniques show massive progress. The number of publications related to various DNA based models and techniques increases tenfold annually. Presented methods literally convert each and every smallest possible information into DNA form. Thus 5 this method is highly applicable for handling and storage of massive amounts of various types of data.

This paper proposes a Novel Technique of Cloud Security Based on Hybrid Encryption by hyper Chaotic logistic bit scrambling schemes, from symmetric block cryptographic and function schemes. In the proposed algorithm performance is analyzed on the basis of two parameters: Storage and time. The Simulation results demonstrate more efficient results in comparison of the obtained parameter output (i.e., storage and time). As encrypts the data through the generation secure data.

Therefore, Chaotic logistic bit has proven to be more efficient that the previous defined algorithm. The future work may lay its emphases on the exploration of the various cryptosystem including encryption algorithm and logistic function. More layers of hybrid function can be included for further increase in the data integrity and security.

File Name	Input File Size (bytes)	Encrypted File Size (bytes)			Encryption Time (ms)			Decryption Time (ms)		
		RSA_MD5	***Blowfish_MD5***	***Logistic Bit scrambling***	***RSA_MD5***	***Blowfish_MD5***	***Logistic Bit scrambling***	***RSA_MD5***	***Blowfish_MD5***	***Logistic Bit scrambling***
Dataset.txt	1216841	2202487	2197245	2159653	186	60	40	123	77	57
new1.txt	581469	1058398	1052530	1050023	95	10	8	44	16	10
new2.txt	581632	1058279	1046018	1037782	120	11	9	47	17	13
new3.txt	378754	687092	685303	683892	77	7	5	38	12	10
new4.txt	1315331	2392053	2380192	2380207	136	27	23	87	33	24

VI. REFERENCES

[1]. C. C. Byers and P. Wetterwald, ‘‘Fog computing distributing data and intelligence for resiliency and scale necessary for IoT: The Internet of Things (ubiquity symposium),’’ Ubiquity, vol. 2015, p. 4, Nov. 2015.

[2]. A. Tumanov, T. Zhu, J. W. Park, M. A. Kozuch, M. Harchol-Balter, and G. R. Ganger. TetriSched: Global rescheduling with adaptive plan-ahead in dynamic heterogeneous clusters. In Proceedings of the Eleventh European Conference on Computer Systems, EuroSys’16, pages 35:1–35:16, New York, NY, USA, 2016. ACM.

[3]. Chandra S, Paira S, Alam SS, Sanyal G (2014) A comparative survey of symmetric and asymmetric key cryptography. In: Proceeding of 2014 International Conference on Electronics Communication and Computational Engineering (ICECCE), IEEE, pp 83–93

[4]. Using Chaotic System in Encryption NASA Astrophysics Data System (ADS)Findik, OÄŸuz; Kahramanli, Åžirzat

[5]. Xu, L., Li, Z., Li, J., & Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 78, 17–25. doi:10.1016/j.optlaseng.2015.09.007

[6]. A combination chaotic system and application in digital data encryption NASA Astrophysics Data System (ADS) Parvaz, R.; Zarebnia, M.

[7]. Security Analysis of a Block Encryption Algorithm Based on Dynamic Sequences of Multiple Chaotic Systems NASA Astrophysics Data System (ADS) Du, Mao-Kang; He, Bo; Wang, Yong

[8]. I.M. Gracia, A.M.R. Aguilera, V. Guerra, J. Rabadan, “Data Sniffing Over an Open VLC Channel,” Proc. of the 10th Int. Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2016 G. M. Church, Y. Gao, and S. Kosuri, “Next-generation digital information storage in DNA,” Science, vol. 337, no. 6102, pp. 1628, 2012.

[9]. Wang C, Wang Q, Ren K. Ensuring data storage security in cloud computing, Cryptology ePrint Archive, Report, 2009 /http://eprint.iacr.org/S [accessed: 18 October 2009].

[10]. D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, “Cloud computing features, issues, and challenges: A big picture,” in Proc. Int. Conf. Comput. Intell. Netw., Jan. 2015, pp. 116–123.