"DATA ENCRYPTION & PRIVACY PRESERVATION IN CLOUD USING CHAOTIC THEORY"

[1]Swapnali S. Tambe, [2]Prof. Sonali A. Patil
PG Student[1], Assistant Professor[2], Department Computer Engineering, JSPM's BSIOTR Wagholi, Pune, India-412207[1, 2]

ABSTRACT: Now days, the chaos-based cryptographic algorithms have attracted a lot of attention. Specially, chaotic tent map (CTM)-based schemes show some good performances in randomness properties and security level. However, several shortcomings still can be found from them. This proposed system is based on the security analysis of the pure CTM-based scheme, proposed a novel image encryption algorithm by using the combination of the rectangular transform and the CTM principle. It encrypts the three channels of the plain image at the same time and these channel encryptions associate with each other. In addition, by generating the key-streams related to both the secret keys and the plain image, its key-sensitivity has been further Improved. This system uses Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that fragments user files into pieces and replicates them at strategic node locations within the cloud. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and the results show that many drawbacks of pure CTM-based schemes have been overcome.

Index Terms: **CTM, DROPS, Image Encryption, Image Decryption.**

I INTRODUCTION

Modern data sharing services are user needs by using new technologies such as cloud of things. The new technology provides more facilities and enhancements to the existing data sharing services as it allows more flexibility in terms of monitoring user's data and remotely connecting with the users via cloud of things. However, there are many security issues such as privacy and security of user's data which need to be considered once we introduce chaotic tent map (CTM)-based schemes to the health care service. In recent years, the chaos-based cryptographic algorithms have attracted a lot of attention. Specially, chaotic tent map (CTM)-based schemes show some good performances in randomness properties and security level.

In this paper, based on the security analysis of the pure CTM-based scheme, we propose a novel encryption algorithm by using the combination of the rectangular transform and the CTM principle. It encrypts the user's data files and then uploading the encrypted data to the cloud for storage and access by user. As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Hence Division and Replication of Data in the Cloud for Optimal Performance and Security(DROPS) methodology is used to divide a file into fragments, and replicate the fragmented data over the cloud nodes. However, efficient and scalable sharing of encrypted data has been a very challenging problem. In addition, by generating the key-streams related to both the secret keys and the files, its key-sensitivity has been further improved. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and our results show that many drawbacks of previous schemes have been overcome.

II LITERATURE SURVEY

A Mahalakshmi, Dr. S. Karthigailakshmi, "An Image Encryption Scheme Based on the Rectangular Transform Enhanced Chaotic Tent Maps", International Research Journal of Engineering Sciences, 2018.

In this work discussed about the image encryption scheme which is based on RT-enhanced CTM. The main intention of this work is to improve the security during image transmission. Initially the input is taken from the dataset. After that the input image is encrypted by using CTM techniques. Then the key is generated for high security purpose. Then the image is encrypted in transmission side. These processes are done in reverse manner when the user decrypts the image. The proposed image encryption technique yields the better results compare to other existing techniques. The main advantage of the work is to offers the high security during data or image transmission and this technique is applied in many security fields [1].

Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai, "Secure Auditing and Deduplicating Data in Cloud", IEEE Transactions on Computers, 2017.

This paper aiming at achieving both data integrity and de-duplication in cloud, which presented SecCloud and SecCloud+. SecCloud introduces an auditing entity with maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. In addition, SecCoud enables secure deduplication through introducing a Proof of Ownership protocol and preventing the leakage of side channel information in data deduplication. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data [2].

C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map", Nonlinear Dynamics, 2017.

In this work discussed about the image encryption scheme which is based on RT-enhanced CTM. The main intention of this work is to improve the security during image transmission. Initially the input is taken from the dataset. After that the input image is encrypted by using CTM techniques. Then the key is generated for high security purpose. Then the image is encrypted in transmission side. These process are done in reverse manner when the user decrypt the image. The proposed image encryption technique yields the better results compare to other existing techniques. The main advantage of this work is to offers the high security during data or image transmission and this technique is applied in many security fields [3].

Jean De Dieu Nkapkop and Joseph Yves Effa, "A Secure and Fast Chaotic Encryption Algorithm Using the True Accuracy of the Computer", Technical University of Cluj-Napoca, Department of Communications, 2016.

This paper, presented a new secure and fast chaos based algorithm for image encryption using the true accuracy of the computer. In the scheme, the permutation-diffusion design based on the fast generation of large permutation and diffusion key with a good level of randomness and a very high sensitivity has been investigated. This procedure allows to use the true accuracy of the computer by using integer sequences obtained by the descending sorting of the Logistic map as a secret key in the permutation stage. This technique avoids the excess digitization of chaotic values [6].

P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining dna coding and entropy", Multimedia Tools and Applications, 2016.

Information security has become more and more important issue in modern society, one of which is the digital image protection. In this paper, a secure image encryption scheme based on logistic and spatiotemporal chaotic systems is presented. The extreme sensitivity of chaotic system can greatly increase the complexity of the presented scheme.

Furthermore, the scheme also takes advantage of DNA coding and eight DNA coding rules are mixed to enhance the efficiency of image confusion and diffusion. To resist the chosen plain text attack, information entropy of DNA coded image is modulated as the parameter of spatio-temporal chaotic system, which can also guarantee the sensitivity of plain image in the encryption process. So even a slight change in plain image can cause the complete change in cipher image. The experimental analysis shows that it cans resistant different attacks, such as the brute-force attack, statistical attack and differential attack. What's more, the image encryption scheme can be easily implemented by software and it was promising in practical application [7].

III EXISTING SYSTEM

Earlier client upload data file on cloud in plain text format. However, there are many security issues such as privacy and security of user's data and wants to maintain the integrity and security on that plain data file. Customers always choose the safest and cheapest method for the data storage and transformation on cloud. But that's not possible to give all features in such minimum amount. Every system has some drawbacks and various problems.

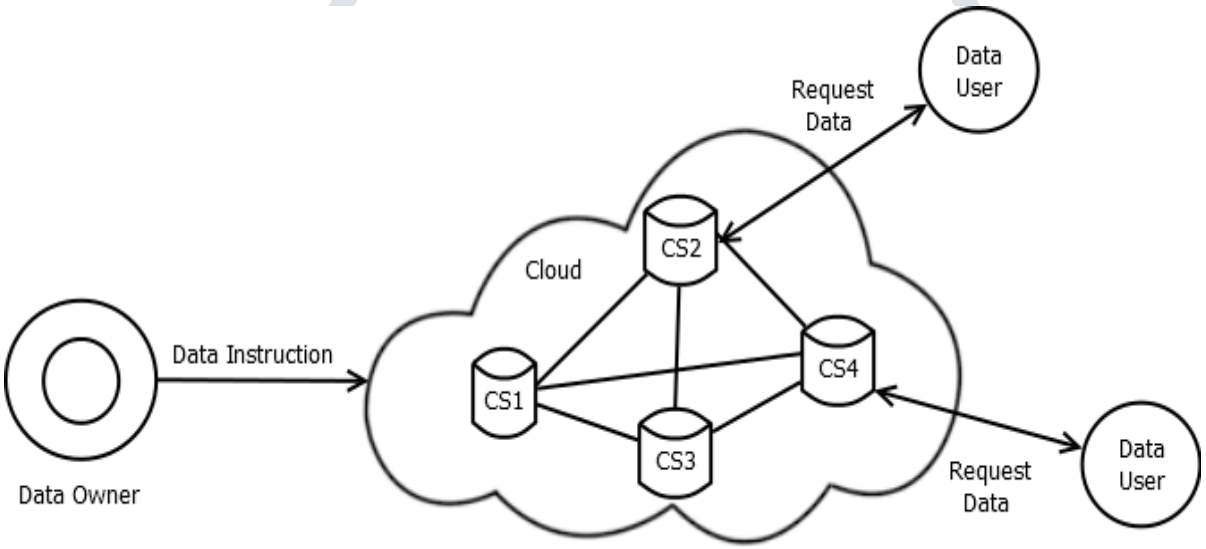

Figure 3.1 Existing System

3.1 Drawbacks of Existing System

1) It is very difficult to audit the files huge and large amount of data in cloud using integrity auditing.
2) Lots of Duplicate files in cloud
3) The number of security problems that are faced by cloud computing are
   - Data issues
   - Privacy issues
   - Infected application

IV PROBLEM STATEMENT

Develop a system which is based on the security analysis of the pure CTM-based scheme, which provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers.

V SYSTEM ARCHITECTURE

In proposed system we introduce chaotic tent map (CTM)-based schemes to the data sharing service. In this project, based on the security analysis of the pure CTM-based scheme, we propose a novel encryption algorithm by using the combination of the rectangular transform and the CTM principle. It encrypts the data files and then uploading the encrypted data to the cloud for storage and access by data user. Division and Replication of Data in the Cloud for Optimal Performance and Security(DROPS) methodology is used to divide a file into fragments, and replicate the fragmented data over the cloud nodes. However, efficient and scalable sharing of encrypted data has been a very challenging problem. In addition, by generating the key-streams related to both the secret keys and the files, its **key**-sensitivity has been further improved. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and our results show that many drawbacks of previous schemes have been overcome.

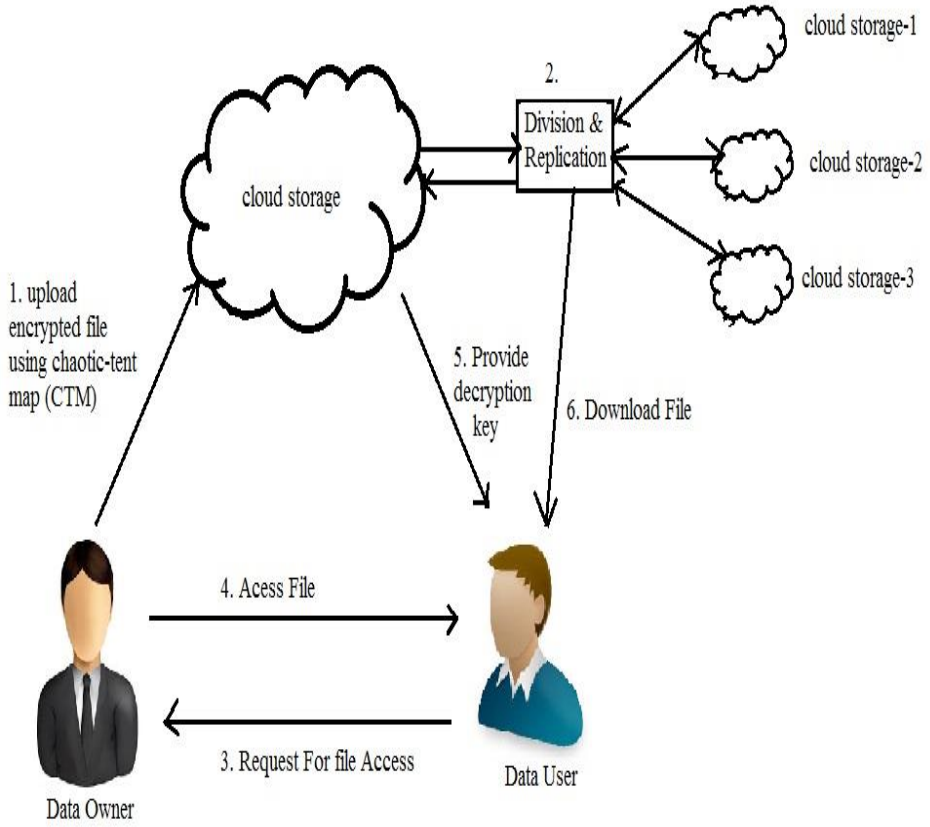

Figure 5.1: System Architecture

VI METHODOLOGY

In this section, we introduce the chaotic cryptography component to generate the key stream iteratively, and to design a discrete chaotic authenticated encryption scheme. The overall architecture of the proposed cryptosystem. First, the internal state is initialized with the key and IV. Then, the associated data are processed optionally. Finally, the cipher-text and authentication tag are generated with plain-text through an iterative internal state update. When deciphering, the same key and IV are used to reconstruct the original plain-text, while no modification is made to the cipher-text; otherwise, a special symbol is used to indicate that the cipher-text is invalid.

6.1 Chaos Theory

Chaos theory concerns deterministic systems whose behavior can be in principle predicted. Chaotic systems are predictable for a while and then appear to become random. The amount of time that the behavior of a chaotic system can

be effectively predicted depends on three things: How much uncertainty can be tolerated in the forecast, how accurately its current state can be measured, and a time scale depending on the dynamics of the system, called the Lyapunov time. Some examples of Lyapunov times are: chaotic electrical circuits, about 1 millisecond; weather systems, a few days (unproven); the solar system, 50 million years. In chaotic systems, the uncertainty in a forecast increases exponentially with elapsed time. Hence, mathematically, doubling the forecast time more than squares the proportional uncertainty in the forecast. This means, in practice, a meaning fulbprediction cannot be made over an interval of more than two or three times the Lyapunov time. When meaningful predictions cannot be made, the system appears random.

6.2 Algorithm: AES Algorithm

1. KeyExpansions
   - For each round AES requires a separate 128-bit round key block plus one more.
2. InitialRound
   - AddRoundKey: with a block of the round key, each byte of the state is combined using bitwise xor.
3. Rounds
   - SubBytes: in this step each byte is replaced with another byte.
   - ShiftRows: for a certain number of steps, the last three rows of the state are shifted cyclically.
   - MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   - AddRoundKey
4. Final Round (no MixColumns)
   - SubBytes
   - ShiftRows
   - AddRoundKey.

VII CONCLUSION AND FUTURE WORK

The chaos-based cryptographic algorithms have attracted a lot of attention. Specially, chaotic theory based schemes show some good performances in randomness properties and security level. This proposed System presents, an image encryption scheme based on RT-enhanced CTM. Its security analysis has also been given in detail. Experimental simulation and performance comparison with other systems show that this new scheme has greatly improved the security while still possessing all the merits of the pure CTM-based schemes, which obviously leads some practical value in implementation. The security of the proposed scheme has been verified by security analysis and experimental evaluations, and our results show that many drawbacks of pure CTM-based schemes have been overcome.

REFERENCES

1) A Mahalakshmi, Dr. S. Karthigailakshmi, “AN IMAGE ENCRYPTION SCHEME BASED ON THE RECTANGULAR TRANSFORM ENHANCED CHAOTIC TENT MAPS”, International Research Journal of Engineering Sciences, 2018.
2) Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai, “Secure Auditing and Deduplicating Data in Cloud”, IEEE Transactions on Computers, 2017.
3) C. Li, G. Luo, K. Qin, and C. Li, “An image encryption scheme based on chaotic tent map”, Nonlinear Dynamics, vol. 87, no. 1, pp. 127133, 2017.

4) Prof.Sonali A. Patil, Dr. Sharmila Sankar, Dr. M. Sandhya, "A survey on cloud computing parameters,"Asian Journal Of Convergence In Technology,volume IV Issue I

5) Prof.Sonali A. patil, Pritam l Mahamne , "A Servey On cloud Data Security And Intigrity using sack of Cryptographic Algoritham through Trusted Third Party(TTP),volume 4,Issue 12,December 2016

6) Prof.Sonali A. patil, Ms.Megha D.savekar, "KNN CLASSIFICATION SCHEME BASED PRIVACY PRESERVATION POLICY OVER SEMANTICALLY SECURE ENCRYPTED DATABASE, IJARIIE-ISSON(O)-2395-4396, vol-2 Issue-3,2016

7) V. Patidar, N. Pareek, and G. Purohit, "A novel quasi group substitution scheme for chaos based image encryption", arXiv preprint arXiv:1709.06270, 2017.

8) A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata", Optics and Lasers in Engineering, vol. 90, pp. 225 237, 2017.

9) Jean De Dieu Nkapkop and Joseph Yves Effa, "A Secure and Fast Chaotic Encryption Algorithm Using the True Accuracy of the Computer", Technical University of Cluj-Napoca, Department of Communications, 2016.

10) P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining dna coding and entropy", Multimedia Tools and Applications, vol. 75, no. 11, pp. 63036319, 2016.

11) L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems", Optics and Lasers in Engineering, vol. 77, pp. 118125, 2016.

12) P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on rgba random image encryption approach", Security and Communication Networks, vol. 8, no. 18, pp. 33353345, 2015.

13) S. Khosla and P. Kaur, "Secure data hiding technique using video steganography and watermarking", International Journal of Computer Applications, vol. 95, 2014.