CREATION OF A CHAOTIC ENCRYPTION GENERATOR USING IMAGES AS ENCRYPTION KEY

Anand V Sunil
Dept.of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Kodakara, India
anand219011@sahrdaya.ac.in

Christeen Jose
Dept.of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Kodakara, India
christeenjose11@gmail.com

Devika M S
Dept.of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Kodakara, India
devika219014@sahrdaya.ac.in

Alan Thomas
Dept.of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Kodakara, India
alan219707@sahrdaya.ac.in

Livya Geroge
Department of Computer Science and Engineering
Sahrdaya College of Engineering and Technology
Thrissur, India
livyageorge@sahrdaya.ac.in

***Abstract*—The importance of randomness in secure encryption cannot be overstated. To prevent attackers from figuring out the encryption key and accessing the data, each new key must be completely random. However, computers are designed to produce predictable outputs based on given inputs, making it challenging to generate random data for encryption keys. With the increasing accessibility of quantum computers, many existing encryption methods are susceptible to being deciphered through brute force. To produce the unpredictable data needed for strong encryption, nature is one of the best sources as it is unpredictable and chaotic. By capturing natural movements with a camera and turning it into an encryption key, we can create unique, completely random data. Encrypted data must appear completely random to prevent attackers from guessing the key used for encryption. Any patterns or predictable values in encrypted data will make it easier for attackers to decipher, rendering it essentially compromised.**

***Index Terms*—Encryption, Cryptography, Video, Capture**

I. Introduction

The secure transfer of data is crucial for a safe and secure cyber environment. It is important to ensure that the data is not intercepted, traced, or viewed. To achieve this safety, secure encryption keys are generated while transferring data. These keys can be created by computer-generated codes or manually. The randomness of the encryption keys is a critical aspect of their security. The new key generated by a computer must be entirely random so that attackers cannot figure out the key and decrypt the data. However, computers are designed to give logical outputs based on a given input, making it challenging to produce the necessary random data for creating unpredictable encryption keys. Human-made encryption keys are also vulnerable to attack as each individual tends to follow an unconscious pattern that can be identified by attackers familiar with advanced cyber attacks. As quantum computers become more accessible, existing encryption methods are becoming easily deciphered. High-speed quantum computers can force their way into data. The solution is to use nature as a source of random data, as it is unpredictable and chaotic, and can produce different unique results each time, even when following a repetitive procedure.The security of data is a significant factor in ensuring a secure cyber environment. It is imperative that the information transmitted is not intercepted, traced, or viewed. To ensure this safety while transferring data, encryption keys are generated for secure communication. These keys are created through either computer-generated codes or human-made methods. The randomness of the encryption keys is critical for secure encryption. Each new key used to encrypt data must be entirely random to prevent attackers from figuring out the key and decoding the data. However, computers are designed to produce predictable outputs based on given inputs, making it challenging to generate random data for unpredictable encryption keys. Human-made encryption keys also pose a significant threat as individuals tend to follow unconscious patterns that can be easily detected by an attacker familiar with advanced cyber attacks such as social engineering. With quantum computers becoming more accessible, many existing encryption methods are easily deciphered. High-speed quantum computers can forcefully enter data. The best option for producing unpredictable and

chaotic data necessary for strong encryption is nature since it is unpredictable and provides various instances where a repetitive process still gives unique results each time.

II. GENERAL BACKGROUND

As the use of more and more powerful supercomputers and quantum computers are increasing the existing methods of data encryption are proving to be vastly inadequate.Highly sought after symmetric encryption techniques like advanced encryption standard which uses 128 and 256 bit keys to narrow down the security threats.But all these are obsolete if an attacker can decrypt the encryption key generated.A cracked or decrypted encryption key is as same as handing over the password.Very sensitive data like classified information or government documents are sometimes encryptrd by hand to increase security.the theory is that humans can be more promising to create random patterns.A machine whenever given the same input will always give back the same output and they can be tricked into replicationg the same output.This was a major flow even in the famed unbreakable code generator 'Enigma' which ultimately led to their defeat.But no matter how random one may think they can generate codes,human mind has a tendency to subconsciously slip into a pattern and a skilled social engineer if given enough time and exposure can mind that pattern.An immediate and effective method is needed to generate truly random encryption key that is not derived from any influence of both machine and man.

A. Problem

The availability of high power computers and networking speeds along with more and more data being stored in digital format has ed to a significant rise in cyber attacks.The current security measures mainly the encryption key generating systems are being cracked and useless at an alarming rate.Even in complex systems with human brain as a center pivot social engineering and other forms of personalized attacks are being used to decipher encrypted cyber data.Therefore a new untraceable and unbreakable security measure is urgently needed to cope with the new wave of online attacks

B. Motivation

The development of encryption technology is an important part of modern information security. To protect the sensitive data from malicious attackers, encryption algorithms must be designed to be unpredictable and secure. Chaotic encryption generation systems provide a powerful tool for developing such algorithms, as they are capable of generating complex and chaotic sequences of random numbers that are difficult to predict or decipher. The use of chaotic encryption algorithms can provide an additional layer of security, as attackers would not be able to guess the encryption key or determine the pattern used to generate the encrypted data. Additionally, chaotic encryption algorithms can help protect data from brute force attacks, as they require significantly more resources and computing power to decrypt than traditional

C. Objectives

The objectives of this work are:

- Providing a high level of security: The aim of any encryption system is to make it difficult for an unauthorized person to access the data being encrypted.
- Improving the efficiency of the encryption process
- Providing flexibility in the encryption process
- Can be customized to meet the specific needs of a given application

III. LITERATURE SURVEY

The study examined effective data access in distributed storage systems while ensuring the recovery of temporarily unavailable nodes and maintaining security. The number of accessible nodes and generated network traffic were used to measure access efficiency, which naturally relates to location and repair bandwidth in the system. The study provided parameter limitations, explicit constructions, and techniques for recovering multiple files simultaneously and distributing the workload across servers during recovery. Challenges, such as considering bandwidth restrictions for small-file recovery and finding optimal codes over tiny fields, were also discussed. The study suggested potential future research areas, including combining efficient access and repair issues.[1]

The exponential growth of digital data has led to serious management issues for users, resulting in the outsourcing of data to cloud servers. Commercial cloud service providers use data deduplication to reduce storage space usage. To address security concerns, a secure password-protected MLE key method called SPADE has been introduced, which includes a proactivization mechanism and a password-hardening protocol. The system is resistant to brute-force and dictionary guessing attacks, and has been proven to be effective in terms of communication and computation expenses. Future work will explore ways to duplicate SPADE's functions without independent key servers and investigate the key management problem. SPADE's strategies can also be applied to similar situations, and the system is compatible with public-key encryption with keyword search (PEKS) schemes for added security.[2]

The use of deep learning models (DLMs) in mobile applications has the potential to offer high-performance cognitive services. However, existing approaches of using edge servers for pre-processing tasks before sending data to cloud servers for analysis have limitations in terms of latency and lack of context-awareness. To address this, a cloud-edge collaboration architecture is proposed in this research, which includes a shallow model (EdgeCNN) on the edge server and a deep model (CloudCNN) on the cloud server. During initialization, EdgeCNN is trained using the lower layers of CloudCNN, while in the updating phase, EdgeCNN is further trained using uploaded data and continuous support from CloudCNN to improve accuracy and reaction times. Additionally, the research also focuses on determining the optimal frequency of retraining and use of edge server resources for EdgeCNN to ensure high accuracy and optimal performance.[3]

Two SEDSSE algorithms can be used in cloud-based medical data to securely and efficiently search for encrypted data. By using medical cloud computing, patients can outsource their medical data to the cloud server and only authorized doctors can access it. With the use of encryption, the sensitive medical data is secured and the corresponding secret key is provided to authorized doctors. However, it is difficult to search encrypted medical data without decryption. The SEDSSE algorithms solve this issue by enabling keyword search over encrypted cloud data, with multi-keyword, fuzzy, and ranked keyword searches. Our schemes outperform previously available works, with effective approaches in terms of storage overhead, index construction, trapdoor generation, and query execution.[4].

Post-Quantum Cryptography (PQC) has become a crucial area of study due to the vulnerability of widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC) to potent quantum computers. Lattice-based, code-based, hash-based, isogeny-based, and multivariate-quadratic cryptography are the most promising cryptosystems according to the National Institute of Standards and and Technology's (NIST) PQC standardisation process. Lattice-based cryptography, particularly Ring-LWE (RLWE) and its recent variation Binary Ring-LWE (BRLWE), is considered a viable option due to its strong security justification, low complexity, and effective implementation. This paper presents two efficient linear-feedback shift register (LFSR)-based architectures for the Inverted Binary Ring-LWE (InvBRLWE)-based encryption technique, one with a parallel-in serial-out structure and the other with a serial-in serial-out structure, that improve upon previously reported designs in terms of area-time complexity. The proposed architectures can be used in various contexts for lightweight application development and are particularly useful for resource-constrained systems.[5]

This study proposes a novel hybrid public/private key cryptography approach based on circular convolution over a collection of ideal Gaussian integer sequences (PGISs) with periods N = pq. The technique uses a trapdoor one-way permutation function known as circular convolution over PGISs to encrypt data with ciphers and create digital signatures. A private PGIS is used as the data encryption sequences, and the decryption key sequence is constructed using a set of private and public keys. The suggested approach has the same level of security as the Rivest-Shamir-Adleman (RSA) system. The method is regarded as a type of hybrid public/private cryptography that benefits from both, as it uses both public and private keys. The approach has a lower computational burden and relies on key exchange mechanisms. The suggested plan strikes a balance among two opposing extremes.[6]

The use of big data in cloud computing applications has raised concerns about privacy. While these technologies have improved service delivery and application performance, the increased volume of data has created challenges in terms of processing and encryption. Many modern programs compromise privacy by foregoing encryption to maintain performance levels. To address this, a Dynamic Data Encryption Strategy (D2ES) has been proposed, which uses cryptographic methods and privacy categorization techniques to enhance privacy protection while adhering to necessary execution time requirements. The D2ES has been tested and found effective in improving privacy. However, unencrypted data transmissions are still a significant concern, and D2ES proposes selective encryption of data to increase the volume of encrypted files while still meeting temporal limitations. This study offers a novel method that selectively encrypts data to optimize privacy protection while meeting big data's speed requirements. The proposed approach can be used with cloud computing's distributed storage systems, and the results of experimental assessments demonstrate the proposed strategy's better and adaptable performance.[7]

Devices for machine-to-machine communication (MTC) are essential in industry 4.0 and the industrial internet of things. These devices are completely automated and support smart factories, healthcare, and surveillance systems. A robust encryption method is required to protect the private information transferred between these devices. Lightweight cryptography has shown to be the best method to deliver the required security for resource-constrained devices. This study provides an in-depth analysis of various types of MTC devices that use hardware- and software-based lightweight cryptography, which are classified according to the suggested system solutions. The essay also provides a taxonomy of lightweight cryptography in M2M communication and offers flexible answers for new advancements.[8]

The security of digital assets is a growing concern for academics and technologists. To address this, a 3D chaotic map-based symmetric technique for multiple pictures is proposed to increase encryption effectiveness and secure transmission. The proposed approach includes four modules: combination, permutation, S-box creation, and substitution using AES iterative methods. The encryption strength of the algorithm is evaluated through assessments of entropy, coefficient of correlation, NPCR, and UACI, as well as the computing time. The proposed method is found to be effective and secure for real-time communication. Other encryption techniques include Recursive Cellular Automata and Deoxyribonucleic Acid for image masking, quantum-color picture masking, aperture fractional order Mellin transform, and neural network-based algorithms. The suggested technique uses a 3D chaotic map for color picture encryption, with four modules combining simple picture row and column permutation, S-box creation, and substitution for permuted pixels to create confusion and diffusion in the image. Experimental results show that the proposed technique has a high encryption effect, strong pixel randomization, and poor correlation of adjacent pixels, making it more secure and appropriate for real-time communication than recent work.[9]

The given data proposes a blockchain-based rights management system that aims to protect the privacy of digital materials, enhance the fairness of copyright transactions, and reduce the time and maintenance burden on digital copyright owners. The proposed system uses a novel multiauthority

ciphertext protocol attribute-based encryption (MA-CPABE) scheme and proxy re-encryption to change ciphertext access policies and sell copyrights to various users. The system employs an Ethereum smart contract for a fair exchange of decryption keys between the rights owner and client, and another blockchain ledger to store data on digital rights. The proposed system provides IND-CPA security, thwarts collusion attempts, safeguards user privacy, and significantly lowers storage costs in public blockchains. It could cut down on the time and management required by artists while ensuring equity of interest between their agents and fans in buying music copyright transactions.[10]

IV. Proposed System

The proposed chaotic encryption system would work by capturing images of random natural events. These images would then be processed using various techniques, such as Fourier analysis or machine learning algorithms, to extract the underlying chaotic dynamics of the system.

Once the chaotic dynamics have been extracted, they can be used to generate a key for encrypting and decrypting data. This key would be unique to each image, meaning that different images would produce different keys.

Sl no.	***Paper***	***Description***	***Efficiency***
1	A Cloud-Edge Collaboration Framework for Cognitive Service	Reduces heavy load caused by huge data sets on hardware of mobile devices.	Uses a secondary shallow edge based CNN over cloud servers that can meet a users fast needs by doing complex multiplication operations.
2	Efficient Hardware Arithmetic for Inverted Binary Ring-LWE Based Post-Quantum Cryptography	An ideal replacement for current simpler cryptographic encryption systems.	Advanced cryptographic method that can resist a quantum attack as well as classic attacks using A Binary ring-LWE and maintains regular load times
3	Secure Codes With Accessibility for Distributed Storage	Reduces large overhead in data needing multiple encrypted nodes to function	Uses a passive eavesdropper to collect all necessary data of user for encrypted file transfer and that cannot be stored after the command is given
4	Secure Password-Protected Encryption Key for Deduplicated Cloud Storage Systems	Increases password hardening and provides suitable defense against replay attacks	Uses multiple services which are implemented in random order using MLE
5	Novel Hybrid Public/Private Key Cryptography Based on Perfect Gaussian Integer Sequences	Can achieve higher confidentiality levels over private key encryption methods.	Uses a circular convolution over perfect Gaussian integer sequences to create an encryption algorithm that also acts as a digital signature
6	Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing	Significantly reduces the encryption time for a set a packages with different time constraints	Uses a D2ES that supports an encryption algorithm to divide and use different data packages for different files with varying time constraints
7	Types of Lightweight Cryptographies in Current Developments for Resource Constrained Machine Type Communication Devices: Challenges and Opportunities	World wide network of smartshops, healthcare and other social workplaces are run securely through various encryption processes	A combination of both lightweight block ciphers and hybrid encryption is used to protect data of users in various social work sections
8	Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption	Improves convenience in transferring digital rights and security of other digital contents of same authors.	A two part blockchain system is proposed with multi-authority ciphertext policy based encryption .
9	Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box	Increases key sensitivity and pixel randomization for better encryption	Uses multiple three dimensional images to create a strong chaotic encryption key based on chaotic map
10	Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data	More efficiency in storage overhead and trapdoor generator and query build.	A practical encryption method against collusion resistance and can ensure backward and forward privacy.

A chaotic encryption generator is a system that uses chaos theory to create a secure, randomly generated key for encrypting and decrypting data. Here is a possible outline of a chaotic encryption generator system:

- Initialization: The system generates a seed value and initializes certain variables, such as the parameters of the chaotic system and the length of the key to be generated.
- Chaotic system: The system uses a chaotic system, such as the logistic map or the Lorenz system, to generate a sequence of numbers that exhibit chaotic behavior. The chaotic system is defined by a set of equations and parameters, which determine the behavior of the system.
- Key generation: The system maps the chaotic sequence of numbers to the desired key length, generating a unique key for each encryption or decryption process.
- Encryption/decryption: The system uses the generated key to encrypt or decrypt data using a symmetric encryption algorithm, such as AES or DES.
- Key storage: The system stores the generated key in a secure location, such as a hardware security module or a secure database.
- Key management: The system manages the key, including generating new keys as needed, revoking keys that are no longer needed, and securely storing and transferring keys between authorized parties.
  By using a chaotic system to generate the key, the chaotic encryption generator system can create a unique, random key that is difficult to predict or reverse-engineer. This makes it a secure method for encrypting and decrypting data.
- Complex and unpredictable key generation and management: The key used for encryption and decryption must be generated and managed in a way that makes it difficult for unauthorized parties to guess or obtain.

CONCLUSION

In conclusion, the use of chaotic encryption generators is an effective approach to providing a secure cyber environment. Randomness is crucial for encryption, and traditional computer-generated and human-made encryption keys have limitations that can be exploited by attackers. Chaotic encryption generators that produce unpredictable and chaotic data offer a more robust and secure method for encryption. The use of nature as a source for producing these chaotic encryption keys offers a promising approach to ensuring secure communication in a world where cyber-attacks are becoming more advanced and prevalent. Overall, chaotic encryption generators provide a reliable and secure means of encryption, ensuring data security in today's digital world.

REFERENCES

[1] L. Holzbaur, S. Kruglik, A. Frolov and A. Wachter-Zeh, "Secure Codes With Accessibility for Distributed Storage," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 5326-5337, 2021, doi: 10.1109/TIFS.2021.3128822.

[2] Y. Zhang, C. Xu, N. Cheng and X. Shen, "Secure Password-Protected Encryption Key for Deduplicated Cloud Storage Systems," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2789-2806, 1 July-Aug. 2022, doi: 10.1109/TDSC.2021.3074146.

[3] C. Ding, A. Zhou, Y. Liu, R. N. Chang, C. -H. Hsu and S. Wang, "A Cloud-Edge Collaboration Framework for Cognitive Service," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1489-1499, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.2997008.

[4] 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.

[5] J. L. Imaña, P. He, T. Bao, Y. Tu and J. Xie, "Efficient Hardware Arithmetic for Inverted Binary Ring-LWE Based Post-Quantum Cryptography," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 69, no. 8, pp. 3297-3307, Aug. 2022, doi: 10.1109/TCSI.2022.3169471.

[6] C. -H. Hsia, S. -J. Lou, H. -H. Chang and D. Xuan, "Novel Hybrid Public/Private Key Cryptography Based on Perfect Gaussian Integer Sequences," in IEEE Access, vol. 9, pp. 145045-145059, 2021, doi: 10.1109/ACCESS.2021.3121252.

[7] K. Gai, M. Qiu and H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," in IEEE Transactions on Big Data, vol. 7, no. 4, pp. 678-688, 1 Oct. 2021, doi: 10.1109/TBDATA.2017.2705807.

[8] S. Ullah, R. Z. Radzi, T. M. Yazdani, A. Alshehri and I. Khan, "Types of Lightweight Cryptographies in Current Developments for Resource Constrained Machine Type Communication Devices: Challenges and Opportunities," in IEEE Access, vol. 10, pp. 35589-35604, 2022, doi: 10.1109/ACCESS.2022.3160000.

[9] M. Tanveer et al., "Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box," in IEEE Access, vol. 9, pp. 73924-73937, 2021, doi: 10.1109/ACCESS.2021.3081362.

[10] J. Gao, H. Yu, X. Zhu and X. Li, "Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption," in IEEE Systems Journal, vol. 15, no. 4, pp. 5233-5244, Dec. 2021, doi: 10.1109/JSYST.2021.3064356.