International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Innovative Self-Encryption Techniques Using Convergent Algorithms for Decentralized Data Security

K. P. Saurabh*[1], Dr. A. R. Raundale*[2]

Received: 28/07/2024 **Revised**: 01/08/2024 **Accepted**: 09/08/2024

Abstract: As computers and communication technologies have become more widespread over the past few decades, the need for digital information protection has surged. Consequently, cryptography has been adopted by nearly all applications that involve data sharing. This technique ensures that messages exchanged between parties remain secure and unreadable at all times. The aim is to maintain data privacy at the network level. Cryptology relies on two main approaches: cryptography and cryptanalysis. Cryptography involves creating methods to encode information so that it cannot be deciphered by unauthorized parties. Various cryptographic techniques have been developed to protect the privacy of data during transmission. This study aims to establish a robust encryption standard to protect user data stored in the cloud.

Keywords: *communication, technologies, Consequently, cryptography, transmission*

INTRODUCTION

Unauthorized users pose a continuous threat to networks, prompting the integration of multiple layers of security into modern network hardware. However, given the immense volume of data constantly traversing the network, relying solely on the security measures of individual devices is often inadequate. Today's networks typically provide data transmission capabilities accessible globally, referred to as "plain text." To enhance protection, cryptography is employed to encrypt data before it is transmitted and decrypt it upon arrival, creating what is known as "cipher text."

Despite the numerous encryption techniques and algorithms available, attackers may still find ways to bypass encryption and revert cipher text to plain text. A common cause of this issue is the data key. For instance, if a string like "How are you?" is encrypted using a key such as XYZ, this key is used for encrypting the entire string. Thus, if an attacker can access this key, even if they only need a small part of the data, they could potentially access the entire encrypted dataset.

CLOUD COMPUTING

Cloud computing represents a groundbreaking approach with the potential to transform how businesses and individuals handle their data. It offers on-demand access to a wide range of computing resources via the Internet. This method of data storage and retrieval presents several benefits, including the provision of superior data services akin to location-independent storage. Unlike traditional computing methods, cloud computing relies on a shared infrastructure and data storage model.

Compared to personal computer use, cloud computing provides enhanced security and privacy. It offers several advantages, such as reduced hardware expenses, flexible on-demand services, and pricing based on actual resource usage. These benefits simplify users' lives by removing the need to manage their own hardware limits. In a multi-tenant cloud environment, users do not have exclusive control over the servers and networks handling their data. This shared access raises concerns about the exposure of sensitive data due to potential malicious attacks, underscoring the importance of taking precautions when storing data in the cloud.

Traditional cryptographic methods are insufficient for protecting cloud data because users lack access to the underlying storage media. Ensuring the security of cloud-based data without relying on local storage is challenging. Verifying the integrity of cloud data involves significant time and effort, particularly due to the high cost of I/O operations. Additionally, the inability to detect data corruption during access and the difficulties associated with restoring deleted data further complicate the process. Checking the accuracy of cloud data can become a time-consuming and costly task, especially when dealing with large volumes of outsourced data and limited user resources.

(Research Scholar Computer Department Dr. Apj Abdul Kalam University, Indore, India)
(Research Supervisor Computer Department Dr. Apj Abdul Kalam University, Indore, India)
Mail id : saurabhnair1344@gmail.com
And arraundale@gmail. Com

SECURITY IN CLOUD

Cloud computing users frequently want to control access to their data while benefiting from the cloud's advantages. They expect to have substantial authority over who can view their information in the cloud. The cloud's computing infrastructure provides on-demand access to data, software, and services. By utilizing these resources on a pay-as-you-go basis, users can avoid the significant initial costs of setting up and maintaining their own IT infrastructure. However, given the absence of physical boundaries in cloud environments, users are understandably concerned about the security of their personal data stored in the cloud. This concern is highlighted by users' reluctance to continue using cloud services if they discover that their data is not securely protected.

PRIVACY PROTECTION IN CLOUD

Due to the critical importance of privacy in data publish-subscribe systems, there has been a decline in trust in cloud servers during the deployment phase. Cloud service providers (CSPs) may share data among themselves or be required to share it with authorized users. The "sticky policy" aims to ensure that the same level of security is upheld when data is transferred from the cloud provider to the user or requester. However, this policy can only be enforced effectively at the receiving end if both the sender and receiver adhere to the same privacy guidelines.

Despite this, there is no universally accepted mechanism to guarantee data privacy. The challenge lies in the lack of a single, standardized language that can accommodate the diverse rule sets of existing policy languages. As a result, there is no globally recognized privacy policy or universal vocabulary for creating privacy safeguards. Various policy languages are available, such as XACMLv2, XACMLv3, PERMIS, P3P, and Keynote, among others. XACMLv2, for example, is less effective in delegation of authority when compared to newer versions like XACMLv3 and PERMIS. While XACML can be used as a policy language for federal regulations, it assumes access to a stateless Privacy-Preserving Data Publication. PERMIS, on the other hand, supports Separation of Duties (SoD) at the state level, accommodating both dynamic and static SoD requirements.

VARIOUS KINDS OF PRIVACY PROTECTION METHODS

Service providers face the difficult task of ensuring that cloud users are authenticated in a way that protects both their privacy and security. Users expect their sensitive personal information, such as financial details or medical records, to be handled with the highest level of confidentiality. To address this, various advanced technologies have been developed, including cryptographic methods, anonymous authentication systems, zero-knowledge proofs, and group signatures, all designed to protect user anonymity while still allowing for necessary identification. CSPs strictly control access, allowing only verified users to interact with the data. The security protocols used by CSPs must be strong enough to prevent any unauthorized access by malicious actors.

Given the large number of users accessing cloud services simultaneously, there is a clear need for more efficient methods that lower the computational demands of these security technologies. There are three key categories of privacy protection techniques that can be used to obscure sensitive data before it is shared publicly.

METHODS RELYING ON ENCRYPTION

Data can potentially be transferred between different service providers with ease. Regardless of its location worldwide, the encryption ensures that the data remains secure. However, the encryption process can be resource-intensive, particularly for the CPU, which may impact overall system performance.

The challenge, therefore, is to find a balance between maintaining robust data security and optimizing system efficiency. To address this, an Enhanced Privacy-Preserving Scheme (EPPS) is designed to improve cloud performance while simultaneously strengthening data security.

DECRYPTION

The issue mentioned earlier is addressed through the use of anonymous Attribute-Based Encryption (ABE) and its extension. Here's how a message encrypted with CP-ABE (anonymous ciphertext-policy attribute-based encryption) can be decoded:

First, the user needs to generate their secret attribute key.

Second, the user must verify that this attribute key aligns with the access control policies. To successfully decrypt the message, the user's attribute linked to the secret key must satisfy the access policy specified in the ciphertext.

DATA ENCRYPTION METHODS

TRIPLE DES

The encryption process begins with a key-independent initial transposition of the 64-bit input data. This is followed by sixteen identical rounds where the data is manipulated based on the key. After these rounds, a left-to-right swap of the last 32 bits occurs, and the final step involves a key-independent transposition of the 64-bit output data. To maintain symmetry during decryption, the sixteen central rounds must be executed in reverse order compared to the encryption process.

In the United States, the NSA has mandated that only 56 bits of key length be used in the DES symmetric block cipher. Of the 32 bits, only 8 are used for parity, while the remaining 24 bits are not utilized. In 3DES, the block size remains 64 bits, but the key length is extended to 112 or 168 bits. When DES was compromised by brute-force and cryptanalytic attacks, 3DES was introduced as a solution to reinforce security without the need to overhaul or replace the DES system.

RSA

RSA (Rivest-Shamir-Adleman) encryption leverages prime numbers to generate a pair of keys: a public key for encryption and a private key for decryption. The public key is used to encrypt information, while the corresponding private key is required to decrypt it, ensuring that only the intended recipient can access the original data.

BLOWFISH

An encryption algorithm with a 64-bit block size and a key length ranging from 32 to 448 bits was developed by Bruce Schneier in 1993. This algorithm, known as Blowfish, was created as a robust alternative to the existing encryption methods DES and IDEA.

OBJECTIVES OF THE STUDY

1. The proposed system aims to deliver a level of secure communication that is nearly unbreakable.

2. Additionally, the system seeks to minimize algorithm complexity to keep operations efficient.

3. The primary goal is to implement this system in IoT devices, anticipating a significant increase in their numbers in the near future.

4. The objective is to create a robust and stable decentralized environment to enhance the utilization of network resources.

5. As indicated by the title, the system seeks to refine the convergence algorithm to make it more adaptable to the network while minimizing processing delays.

PROPOSED FRAMEWORK

A) During data transfer, the number of characters in each word is alternately incremented by X and Y.

For example:

Let X be 60 => odd wordsLet Y be 70 => even words

B) First ‘n’ bits are always garbage bits based on time

stamp.For example:

If the time stamp is 2022-08-30 12:36:23.322Then,

The number of garbage bits is 2+0+2+2+0+8+3+0+1+2+3+6+2+3+3+2+2 = 41 garbage bits.

i.e. the first 41 bits can be some random bits.

C) Since the initial bits are generated randomly, an intruder cannot access the data until all the bits have been compromised. With a sufficiently long key, AES encryption of the HEADER—containing the timestamp—ensures that brute-force decryption would take hundreds of years with current technology.

ENCRYPTION

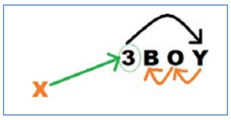
PLAIN TEXT:

BoY

DATA TO BE SENT : 3BoY (It indicates that the data needs to be broken after

3packets where each packet contains 1 character)

ENCRYPTION SEQUENCE:



STEP1: ENCRYPT Y with 3

Y	3	Y XOR 3 (output4)
0	0	0
1	0	1

0	0	0
1	0	1
1	0	1
0	0	0
0	1	1
1	1	0

STEP2: ENCRYPT o with Y

o	Y	o XOR Y (output3)
0	0	0
1	1	0
1	0	1
0	1	1
1	1	0
1	0	1
1	0	1
1	1	0

STEP3: ENCRYPT B with O

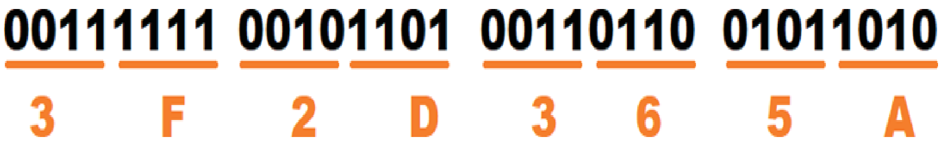
B	o	B XOR o (output2)
0	0	0
1	1	0
0	1	1
0	0	0
0	1	1
0	1	1
1	1	0
0	1	1

STEP4: ENCRYPT 3 with X

As given above, let X=60,Therefore;

60+3=63 i.e. 00111111

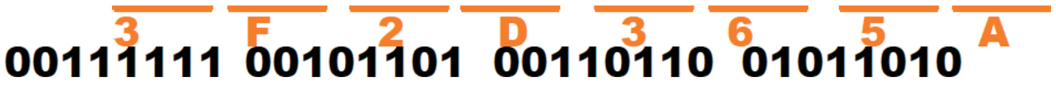
Data to be sent:



CIPHER TEXT : 3F2D365A

DECRYPTION

CIPHER TEXT : 3F2D365A



You may think of data packets as a series of random bits that have been assigned atime stamp.

The first 8 bits here should indicate the data's length. i.e. 00111111 => 63

Given that this is the first word in the series (an odd number), we may deduce that X=60. As a result, 63 minus 60 equals 3.

Therefore, there are 3 units of data.

With a cut-off length of 3, the information may be found in the following three 8-bitpackets. Some more random data might be sent after those three packets.

Sending packets P1, P2, and P3 are good names.

STEP1: DECRYPT P3 with 3

P3	3	P3 XOR 3
0	0	0
1	0	1
0	0	0
1	0	1
1	0	1
0	0	0
1	1	0
0	1	1

i.e. P3 XOR 3 => Y

STEP2: DECRYPT P2 with P3 XOR 3

P2	P3 XOR 3	P2 XOR (P3 XOR 3)
0	0	0
0	1	1
1	0	1
1	1	0
0	1	1

1	0	1
1	0	1
0	1	1

i.e. P2 XOR (P3 XOR 3) => o

STEP3: DECRYPT P1 with P2 XOR (P3 XOR 3)

P1	P2 XOR (P3 XOR 3)	P1 XOR (P2 XOR (P3 XOR 3))
0	0	0
0	1	1
1	1	0

0	0	0
1	1	0
1	1	0
0	1	1
1	1	0

i.e. P1 XOR (P2 XOR (P3 XOR 3)) => B So, ultimately we obtained BoY as plaintext.

CONCLUSION

Data security is a top priority for service providers. Cloud environments can be used to securely generate, store, and manage cryptographic keys, ensuring that only authorized entities have access. However, the rise of Internet technology has led to an increase in sophisticated attacks, posing significant challenges for service providers in protecting their customers' personal and business data. The primary concerns are user authentication and data protection, as malicious actors may steal and misuse user data. Although there are identity management solutions available in the cloud, they do not guarantee complete data security. High-quality encryption standards are essential for ensuring robust data protection.

Encryption algorithms are vital for securing digital communications, but they can be resource-intensive and slow. This study evaluates the AES and DES encryption methods. Experimental results show that DES requires less time and memory for encryption, while AES, though using less memory, takes slightly longer overall. The primary goal of this study is to identify and address common issues in electronic communication. Cryptography remains a key solution for mitigating internet security risks, where the transmitter uses a key to encrypt plain text and the receiver uses the same or a different key to decrypt it, thereby protecting sensitive and public information from unauthorized access.

References :

[1] Gupta, Rajeev & Almuzaini, Khalid & Pateriya, R. & Shah, Kaushal & Shukla, Piyush & Akwafo, Reynah. An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large-Scale 5G. Wireless Communications and Mobile Computing. 2022. 1-14. 10.1155/2022/7291250, (2022).

[2] Basha, A. & N, Rajkumar & AlZain, Mohammed & Masud, Mehedi & Abouhawwash, Mohamed. Fog-based Self-Sovereign Identity with RSA in Securing IoMT Data. Intelligent Automation & Soft Computing. 34. 1693-1706. 10.32604/iasc.2022.024714, (2022).

[3] Solanki, Luv & Chaudhary, Marmik & Chudasama, Dhaval & Chaudhary, Sumit. A Comparative Study of Hybrid Network Security. 8. 333-338, (2022).

[4] Samanta, Debabrata & Alahmadi, Ahmed & Khan, Mohammad & Banerjee, Amit & Dalapati, Goutam & Ramakrishna, Seeram. Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture. IEEE Access. PP. 10.1109/ACCESS.2021.3095297, (2021).

[5] Aruna, M & Mohammad, • & Hasan, Mohammad & Islam, Shayla & Mohan, • & Preeta, • & Hassan, Rosilah. Cloud to cloud data migration using self- sovereign identity for 5G and beyond. Cluster Computing. 10.1007/s10586-021- 03461-7, (2021).

[6] Loukil, Faiza & Ghedira, Chirine & Boukadi, Khouloud & Benharkat, Aïcha- Nabila. Privacy-Preserving IoT Data Aggregation Based on Blockchain and Homomorphic Encryption. Sensors. 21. 2452. 10.3390/s21072452, (2021).

[7] Li, Xiaoyun & Zheng, Zibin & Dai, Hong-Ning. When services computing meets blockchain: Challenges and opportunities. Journal of Parallel and Distributed Computing. 150. 1-14. 10.1016/j.jpdc.2020.12.003, (2021).

[8] Kaur, Manpreet & Gupta, Shikha. Blockchain Technology for Convergence: An Overview, Applications, and Challenges. 10.4018/978-1-7998-6694-7.ch001, (2021).

[9] Naser, s. CRYPTOGRAPHY: FROM THE ANCIENT HISTORY TO NOW, IT'S APPLICATIONS AND A NEW COMPLETE NUMERICAL MODEL. 10.13140/RG.2.2.13438.51524,(2021).

[10] Meraouche, Ishak & DUTTA, Sabyasachi & Tan, Haowen & Sakurai, Kouichi. Neural Networks Based Cryptography: A Survey. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3109635, (2021).

[11] Ahmad Jan, Mian & Cai, Jinjin & Gao, Xiang-Chuan & Khan, Fazlullah & Mastorakis, Spyridon & Usman, Muhammad & Alazab, Mamoun & Watters, Paul. Security and Blockchain Convergence with Internet of Multimedia Things: Current Trends, Research Challenges and Future Directions. Journal of Network and Computer Applications. 175. 102918. 10.1016/j.jnca.2020.102918, (2021).

[12] Abbas, Khizar & Tawalbeh, Loai & Rafiq, Ahsan & Muthanna, Ammar & Elgendy, Ibrahim & Abd El-Latif, Ahmed. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities. Security and Communication Networks. 2021. 1-13. 10.1155/2021/5597679, (2021).

[13] Ranathunga, Tharindu & McGibney, Alan & Rea, Susan. The convergence of Blockchain and Machine Learning for Decentralized Trust Management in IoT Ecosystems. 499-504. 10.1145/3485730.3493375, (2021).

[14] Abubaker, Zain & Khan, Asad & Almogren, Ahmad & Abbas, Shahid & Javaid, Atia & Radwan, Ayman & Javaid, Nadeem. Trustful Data Trading through Monetizing IoT Data using BlockChain based Review System. Concurrency and Computation Practice and Experience. 10.1002/cpe.6739, (2021).

[15] Lissiyas Antony & Dr. Sobhana N V A Review Paper on Securing Surveillance Data using Incremental Cryptography International Journal of Engineering Research & Technology (IJERT) Vol. 10 ISSN: 2278-0181, 2021