Organized Added Shield near Complete Movement Chunk Cryptographic Scheme

[1]Dr. K. Srilatha, [2] Ganesh Khekare
Affiliations(s):
[1]*LGPR Post Doctoral Candidate, Lincoln University College, Malaysia.*
[2] *School of CSE, Vellore Institute of Technolog, India.*

Abstract

Through the rapid progress of converted internet movement, confirming safety but keeping perceptibility takes converted a serious task popular recent web schemes. A Organized Added Shield agenda unified through cryptographic organizations near do smart movement obstructive. The scheme syndicates encryption methods, movement grouping, then irregularity exposure near avoids wicked facts run. Scientific showing exists recycled toward value arrangement presentation, encryption asset, then recognition precision. The training is maintained through perceptions.

Keywords: Chunk Encryption, Dynamic Keying, Secure Transmission, Organized Added Shield.

1. Introduction

The growth of virtual pressures has completed cryptography a important module of system safety. Current setups trust seriously arranged encoded procedures such as TLS and HTTPS, creation circulation examination tough. Most of the network transportation stays encoded, which confuses outdated checking then risk discovery devices .

The test deceits popular matching in Privacy, Safety observing, Present delaying of mean movement.

2. Literature Review

Numerous cryptographic move toward contain be planned toward advance information safety:

Mass symbols scheme:

Mass symbols such as AES plus 3DES be extensively utilized encryption principles. They work on top of permanent volume mass (normally 64 or else 128 bits) plus rely resting on uncertainty plus distribution values.

Trivial Cryptography

Trivial mass symbols be planned intended for forced situations similar to IoT. These comprise SPN, Feistel, plus ARX arrangements, contribution effectiveness plus compact control utilization.

ML support Cryptographic classification

Current workings center going on recognize encryption algorithms by numerical plus ML methods.

Multi layer Encryption methods

Current scheme use multi-layer encryption intended for improved safety within confuse memory schemes.

Presented methods require:

- capable portion mobility usage
- Adaptive protecting method
- mixing of planned group by encryption

Problem Statement

Despite advancements, current cryptographic schemes suffer from:

1. **Static Block Processing**
   Fixed-size encryption does not adapt to dynamic data streams.
2. **Security Weakness in Repetitive Patterns**
   Identical plaintext blocks produce identical ciphertext in certain modes.
3. **High Computational Cost**
   Complex encryption layers increase latency.
4. **Lack of Mobility Awareness**
   Data chunks are not dynamically reorganized during encryption.

Projected scheme: OAS-CMCCS

The proposed scheme introduces three key components:

1. **Organized Chunk Division**
2. **Added Shield Layer**
3. **Complete Movement Mechanism**

Scheme Design:

Plaintext → Chunk Division → Chunk Movement → Shield Layer Encryption → Ciphertext

Mathematical Model

Let:

- MMM = plaintext message
- CiC_iCi = chunk i
- KiK_iKi = dynamic key
- SiS_iSi = shield transformation
- E()E()E() = encryption function

Step 1: Chunk Division

M={C1,C2,C3,...,Cn}M = \{C_1, C_2, C_3, ..., C_n\}M={C1,C2,C3,...,Cn}

Step 2: Dynamic Key Generation

Ki=H(Ki−1⊕Ci)K_i = H(K_{i-1} \oplus C_i)Ki=H(Ki−1⊕Ci)

Where HHH is a hash function.

Step 3: Chunk Movement Function

Ci′=f(Ci,i)=C(i+σ)mod nC_i' = f(C_i, i) = C_{(i + \sigma) \mod n}Ci′=f(Ci,i)=C(i+σ)modn

Where:

- σ\sigmaσ = shift parameter

Step 4: Shield Layer Transformation

Si=Ci′⊕Ki⊕RiS_i = C_i' \oplus K_i \oplus R_iSi=Ci′⊕Ki⊕Ri

Where RiR_iRi is a random nonce.

Step 5: Encryption

Ei=E(Si,Ki)E_i = E(S_i, K_i)Ei=E(Si,Ki)

Final Ciphertext

C={E1,E2,...,En}C = \{E_1, E_2, ..., E_n\}C={E1,E2,...,En}

Security Analysis

Resistance to Known Attacks

Attack Type	**Confrontation**
Brute Force	High (dynamic keys)
Replay Attack	Prevented via nonce
Pattern Attack	Eliminated via chunk movement
Statistical Attack	Reduced entropy leakage

Presentation valuation

Evaluate by conventional schemes:

Parameter	**AES**	**Proposed Scheme**
Plasticity	Low	High
Safety level	Single	Multi-layer
Chunk management	Static	Dynamic
Competence	Medium	High

Future scope

The planned OAS-CMCCS system can exist extensive within a number of customs:

1. Addition by AI-based input invention
2. Post - Quantum Cryptography version
3. Hardware execution intended for IoT procedure
4. Chunk chain-based protected Chunk confirmation
5. Modification intended for immediate cartridge Encryption

Upcoming study inside post-quantum safety places of interest the significance of intensification symmetric cryptographic reproduction.

Conclusion

This paper initiate the **Organized Added Shield near Complete Movement Chunk Cryptographic Scheme**, a fresh advance to augment conventional chunk encryption method via add in portion association plus covered protecting. The planned replica talk to boundaries of stationary encryption scheme plus supply better protection, scalability, in addition to flexibility. Statistical representation plus study show its use within current circulated surroundings.

References

1. Ellis, S. R., *Computer and Information Security Handbook*, 2013.
2. Andress, J., *The Basics of Information Security*, 2011.

3. Gilchrist, J., *Encyclopedia of Information Systems*, 2003.
4. Rana, M. et al., “Lightweight cryptography survey,” 2022.
5. Cheng, C. W. et al., “Block Encryption Schemes Analysis,” 2022.
6. Wu, H. et al., “Cryptographic Identification,” 2015.
7. B. Momjian, PostgreSQL: introduction and concepts. Addison-Wesley New York, 2001, vol. 192.
8. T. Müller and F. C. Freiling, “A systematic assessment of the security of full disk encryption,” IEEE TDSC, pp. 491–503, 2014.
9. NVM Express, “NVMExpress Base Specification Revision 1.4,” 2019
10. A. S. Rakin, M. H. I. Chowdhuryy, F. Yao, and D. Fan, “Deepsteal: Advanced model extractions leveraging efficient weight stealing in memories,” IEEE Security and Privacy, pp. 1157–1174, 2022.
11. B. Rogers, S. Chhabra, M. Prvulovic, and Y. Solihin, “Using address independent seed encryption and bonsai merkle trees to make secure processors os-and performance-friendly,” in IEEE MICRO, 2007, pp. 183–196.
12. G. Saileshwar, P. J. Nair, P. Ramrakhyani, W. Elsasser, J. A. Joao, and M. K. Qureshi, “Morphable counters: Enabling compact integrity trees for low-overhead secure memories,” in IEEE MICRO, 2018, pp. 416–427.
13. G. Saileshwar, P. J. Nair, P. Ramrakhyani, W. Elsasser, and M. K. Qureshi, “Synergy: Rethinking secure-memory design for error-correcting memories,” in IEEE HPCA, 2018, pp. 454–465.
14. Samsung, “Ultra-Low Latency with Samsung Z-NAND SSD,” Samsung Memory Solutions Lab, Tech. Rep., 2017.