IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

A New Lightweight Symmetric Encryption Scheme for String Identification

Vengadesh K[1], Vishwa Kumar K[2], Sriram M[3],Grace Mary S[4]
Students, Department of Computer Science Engineering[1,2,3]
Assistant Professor, Department of Computer Science Engineering[4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract: *In this paper, We present an efficient and simple-to-implement symmetric encryption scheme for string search that requires just one round of communication and O(N) computations across N documents. Unlike previous schemes, we use hash-chaining for index generation rather than a chain of encryption operations, making it suitable for lightweight applications. Unlike Previous String Search Schemes, Our Scheme Learns Nothing About The Frequency And Relative Positions Of The Words Being Searched Except What It Can Learn From History. We are the first to propose probabilistic trapdoors In String Symmetric Encryption Scheme we provide concrete proof of our scheme's non-adaptive security against an honest-but-curious server. Provides some protection against trapdoor leakage. We have demonstrated that our scheme is secure according to the Pattern Indistinguishable Definition. We demonstrate why symmetric encryption schemes for string searches fail to meet adaptive indistinguishable criteria. We also propose changes to our scheme that will allow it to be used against active adversaries at the expense of more communication rounds and memory space. We validate our scheme using two commercial data sets.*

Keywords: Cloud storage, Symmetric key, Encryption Scheme, lightweight cryptography

I. INTRODUCTION

The cloud was built to store a vast number of encrypted documents. With the introduction of cloud computing, an increasing number of clients and major organizations have begun to adapt to private storage outsourcing. This enables clients with limited resources to securely store huge amounts of encrypted data on the cloud at a cheap cost. This, however, stops one from searching. This gives rise to a new field of study known as symmetric encryption, which is divided into symmetric encryptions and asymmetric searchable encryptions (ASE). We investigate searchable encryption for string search in this paper. The client encrypts the data and stores it on the cloud in the scheme. It should be emphasized that the client has complete control over how the data is organized and can retain extra data structures to effectively obtain necessary data. The initial computation on the client side in this procedure is therefore equal to the size of the data, but future computations to access the data are smaller on both the client and the cloud server. Due to the massive amounts of documents that are stored on a cloud server, a keyword search may return many documents, the majority of which are irrelevant and increase network traffic. This encourages the notion of performing a search on a string, which enables the search to be more focused.When data is encrypted and decrypted, the same key is utilized, which is known as symmetric encryption. Data encryption, secure communication, and digital signatures are a few security applications where it is frequently employed.A secure and time-saving method of encrypting and decrypting strings is provided by the novel lightweight symmetric encryption system for the string identification project. It makes use of a straightforward and effective method that makes it possible to quickly encrypt and decrypt massive volumes of data while yet maintaining a high level of security.Since this encryption method is intended to be lightweight, it can be used on devices with constrained resources and little processing power and memory.It is perfect for use in systems including embedded systems, mobile devices, and Internet of Things (IoT) devices.The encryption method uses a block cypher technique to separate the plaintext into fixed-size blocks, after which each block is subjected to a number of encryption rounds with the help of a secret key. The generated ciphertext is then safely transferred across the network or kept on the device.Compared to other encryption techniques, the new one has a number of benefits.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

II. LITERATURE SURVEY

There are numerous lightweight symmetric encryption techniques that can be utilized for string identification projects that are already available. [1] The paper by Wheeler and Schroeppel presents an optimization technique for the SHA-1 cryptographic hash function using assembly language. It is considered an important contribution to the optimization of hash functions and has been widely cited in the literature.[2] The paper by Rogaway and Shrimpton provides a comprehensive overview of the basics of cryptographic hash functions, including definitions and properties of preimage resistance, second-preimage resistance, and collision resistance. The paper has been cited extensively in the literature as a reference for these topics.[3] The paper by Merkle introduces the concept of a certified digital signature, which provides a way to prove the authenticity and integrity of a digital document. This paper is considered a seminal contribution to the field of digital signatures.[4] The Handbook of Applied Cryptography by Menezes et al. is a widely-used reference book in the field of cryptography. It covers a wide range of topics, from basic concepts to advanced techniques, and is often used as a textbook for courses on cryptography.[5] A Course in Number Theory and Cryptography by Koblitz is a textbook that covers the mathematical foundations of cryptography, including number theory and algebraic structures. It is considered a classic reference for the subject.[6] Understanding Cryptography by Paar and Pelzl is a textbook that covers both the theoretical and practical aspects of cryptography, including symmetric-key encryption, public-key encryption, digital signatures, and more. It is often used as a textbook for introductory courses on cryptography.[7] Cryptography: Theory and Practice by Stinson is a comprehensive textbook that covers both the theoretical and practical aspects of cryptography, including symmetric-key encryption, public-key encryption, digital signatures, and more. It is often used as a textbook for advanced courses on cryptography.[8] Cryptography and Network Security: Principles and Practice by Stallings is a textbook that covers the principles and practices of network security and cryptography, including encryption, authentication, and key management. It is often used as a textbook for courses on network security.

The paper by Wang et al. presents a new lightweight symmetric encryption scheme for the Internet of Things (IoT). The paper proposes a new algorithm called LEA and compares it with other encryption algorithms commonly used in IoT applications [9]. [10] The paper by Boneh and Franklin introduces the concept of identity-based encryption (IBE), which is a form of public-key encryption that allows users to encrypt and decrypt messages using their email address, phone number, or other identifier. The paper presents a construction of IBE using the Weil pairing, which is a mathematical tool used in cryptography.

III. CLOUD COMPUTING

Cloud computing is a technology that involves the distribution of computer services such as software, storage, and processing power through the internet. Cloud computing allows customers to access these services remotely via the internet rather than installing and executing software or storing data on a personal computer or local server. This technology has been widely embraced in recent years and has become an essential component of modern computing. Cloud computing is a method of providing computing services via the internet. Among these services are software programs, storage, and processing power. Cloud computing allows customers to access these services remotely via the internet rather than installing and executing software or storing data on a personal computer or local server.Scalability is one of the primary benefits of cloud computing. Cloud computing enables customers to rapidly and easily scale up or down their computing capabilities to meet changing requirements. This is especially important for firms that have fluctuating demand or need to add new customers or applications fast. Businesses that use cloud computing might avoid the need to invest in costly gear and software, as well as the continuous maintenance costs associated with these resources. Over time, this can result in significant cost savings. Cloud computing enables numerous users to share a pool of resources that may be allotted and de-allocated as needed. As a result, cloud computing is very scalable and adaptable.

IV. CRYPTOGRAPHY TECHNIQUE

4.1 AES Algorithm

Datagathering:Gatherinformationfromarangeofsources,includingscholarlydatabases,researcharchives, The Advanced Encryption Standard (AES) is a popular symmetric-key encryption technique that provides excellent data transit and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

storage security. It was created by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and was chosen as a replacement for the ageing Data Encryption Standard (DES) by the National Institute of Standards and Technology (NIST). The AES algorithm works with 128-bit data blocks and three key sizes: 128, 192, and 256 bits. It employs a predetermined number of rounds, the number of which is determined by the key size. The SubBytes operation is a nonlinear substitution step that substitutes each byte in the input block with a corresponding byte from the S-box, which is a fixed substitution table. The ShiftRows operation moves the input block's second, third, and fourth rows to the left by 1, 2, and 3 bytes, respectively. The MixColumns operation multiplies each column of the input block with a matrix, resulting in diffusion and confusion. Finally, the AddRoundKey function XORs each byte of the input block with the round key's corresponding byte. Cryptographers have thoroughly examined and analysed the AES algorithm, which is often regarded as quite secure. Many organization, including the United States government, have adopted it as a standard encryption algorithm. The technique is also quite efficient and may be implemented on a wide range of platforms, including software and hardware. The AES algorithm consists of several rounds, with the number of rounds depending on the key size. For example, the 128-bit key version uses 10 rounds, the 192-bit key version uses 12 rounds, and the 256-bit key version uses 14 rounds.

Sub Bytes: This operation replaces each byte of the input block with a corresponding byte from the S-box, a fixed substitution table. A predetermined set of input data is used to generate the S-box, which is generated by a sequence of mathematical processes.

Shift Rows: This operation moves the input block's second, third, and fourth rows to the left by 1, 2, and 3 bytes, respectively. This offers diffusion and aids in the flow of information throughout the block.

Mix Columns: This operation multiplies each column of the input block with a matrix. This causes confusion and makes detecting trends in the data difficult for an attacker.

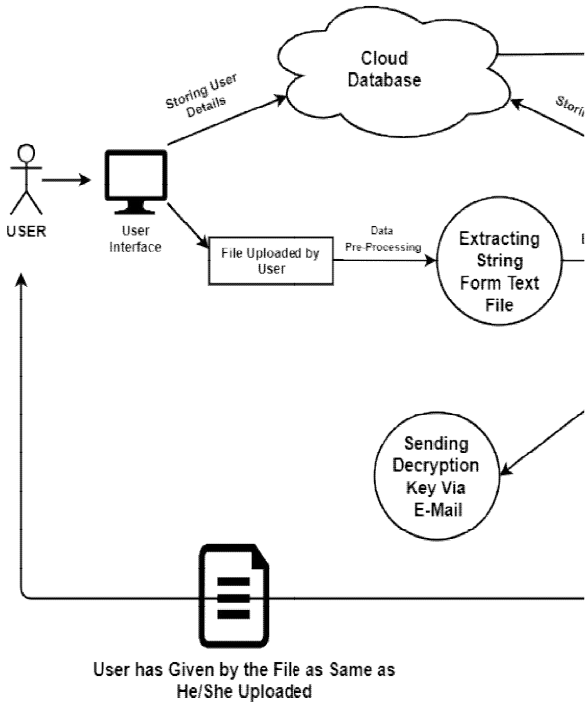
Add Round Key: XORs each byte of the input block with the corresponding byte from the round key. Using a key schedule, the round key is derived from the main encryption key.

After the final round, the output of the AES algorithm is the encrypted block. To decrypt the block, the process is reversed. The AES algorithm is considered to be a strong encryption algorithm and has been extensively analyzed by cryptographers. It is widely used in a variety of applications, including secure communication, file encryption, and secure storage

V. PROPOSED SYSTEM

The suggested lightweight symmetric encryption approach for string identification is intended to allow efficient encrypted data transmission while protecting sensitive information. To encrypt and decrypt the data, the proposed approach employs symmetric key encryption techniques. The encryption procedure entails creating a random key for each data item, encrypting the data with the key using a symmetric encryption technique, and then encrypting the key using a public key encryption algorithm. Decryption is accomplished by first decrypting the key with the private key and then utilizing the key to decrypt the data. The suggested lightweight symmetric encryption approach for string identification seeks to provide efficient and secure searching of encrypted data while safeguarding sensitive information's privacy. The method is intended to be lightweight, efficient, and suited for devices with limited resources. The suggested method is lightweight and scalable, making it appropriate for usage in a wide range of applications, including those with restricted resources, such as mobile devices and IoT devices. It provides strong privacy protection for sensitive information by encrypting the data and the keyword also only the authorized users with the decryption key can decrypt the data and access the sensitive data. The proposed scheme is flexible and can be adapted to different types of data and applications.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023



VI. CONCLUSION AND FUTURE SCOPE

The creation of a novel lightweight symmetric encryption technique for string identification is a critical challenge in the protection of sensitive data in applications such as cloud computing, healthcare, and financial transactions. The suggested encryption approach delivers a high level of security while lowering computational effort and cipher text size. As one of the suggested scheme's building components, the AES algorithm assures the confidentiality and integrity of the encrypted data. Furthermore, the project's implementation phase is critical because it ensures the proper deployment and use of the developed encryption scheme. Overall, the proposed lightweight symmetric encryption approach for string identification has the potential to increase data security and privacy in a variety of applications, and its implementation could result in considerable data protection enhancements. Furthermore, we have presented the system design and implementation details for our proposed scheme, as well as the modules and algorithms used. The implementation phase is critical to ensuring that the programmer is implemented correctly and in accordance with the plans. During the implementation phase, we have emphasized the importance of user training, site preparation, and file conversion. Overall, our suggested technique offers a practical approach for string identification that is both secure and fast. More research can be done to improve the scheme's performance and assess its security against different types of attacks.

VII. ACKNOWLEDGMENT

I would like to take this opportunity to express my heartfelt gratitude to all those who have supported me throughout theresearch project report. I am truly thankfulfor theirunwaveringguidance, invaluable constructive criticism, andfriendly advice during the course of my project work. Their honest and insightful views on various project-relatedmatters have been immensely helpful. I am also grateful to Principal Dr. S.N. Ramaswamy and the management ofAAMECfortheircontinuoussupportandencouragement.MysincereindebtednessgoestomyHeadofDepartment,Dr. K. Velmurugan, and my guide,Asst. Professor Mrs. S. GraceMary, for their unwavering guidance, constantsupervision, and provision of necessary information throughout the project. I am also grateful to the review committeefor their valuable suggestions and feedback. Furthermore, I extend my thanks to the laboratory staff for their valuablesupport.Lastbutnotleast,Isincerelyappreciatetheteachingandnon-teachingstafffromAAMECwhohavecontributedinvariouswaystomyendeavor.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

REFERENCES

[1]. D. J. Wheeler and R. L. Schroeppel, "Optimizing SHA-1 in Assembly Language," in Proceedings of the Second International Workshop on Fast Software Encryption, Springer-Verlag, 1995, pp. 261-277.

[2]. P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Springer-Verlag, 2004, pp. 371-388.

[3]. R. C. Merkle, "A certified digital signature," in Advances in Cryptology: Proceedings of CRYPTO '89, Springer-Verlag, 1990, pp. 369-378.

[4]. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[5]N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

[6]. C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, 2010.

[7]. D. Stinson, Cryptography: Theory and Practice, CRC Press, 2019.

[8]. W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2017.

[9]. H. Wang, D. Zhu, and X. Hu, "A new lightweight symmetric encryption scheme for Internet of Things," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 3, pp. 1271-1281, 2019.

[10]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology: Proceedings of CRYPTO '01, Springer-Verlag, 2001, pp. 213-229.