iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.56957

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

Data Rakshak

Dombale Anita[1], Andure Sidhant[2], Anand Asit[3], Naphade Amit[4], Sharma Ananya[5], Andhale Aditya[6], Andraskar Shruti[7]
Department of Engineering, Sciences and Humanities (DESH) Vishwakarma Institute of Technology, Pune, 411037, Maharashtra, India

Abstract: ***Information security is essential as data exchange moves towards an electronic system. In today's visual communication system, picture, text, and video protection are crucial. Unauthorized uses of private videos, text, and image data must be prevented. It can be difficult to find and identify unauthorized users. Several researchers have proposed several methods for protecting the transfer of texts. We created an encryption and decryption technique with security in mind. We have primarily concentrated on data security, which may be utilized by security agencies, the IT sector, SMBs, the healthcare industry, governmental organizations, the legal industry, financial and banking institutions, etc.***
Keywords: Decryption, Image/Video Encryption, Image/Video/Text, decryption Algorithm and Encryption Algorithm

I. INTRODUCTION

Numerous applications on the Internet for digital communication have seen a noteworthy and ongoing development. Therefore, it is necessary to offer secure communication sessions. Data security as it is transmitted over a worldwide network is now taken into account heavily while evaluating network performance. In order to prevent eavesdroppers from accessing and utilising transmitted data, the privacy and reliability of data are required.

Around 170 incidences of data theft were recorded in India in 2021. The number of cyber-crimes involving the theft of data increased significantly from the previous year. Growing digital use and a lack of awareness of cyber security may be two significant reasons contributing to the rise in cybercrime in the nation.

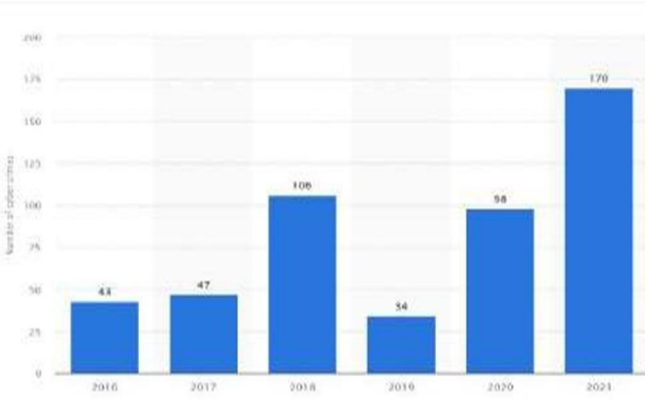


Fig 1: - Data survey for online frauds

A. Encryption

Encryption, a mathematical strategy that employs one or more cryptographic procedures, protects digital data. The data entered is rendered unreadable through encryption because an algorithm converts the plaintext (original text) into ciphertext (an alternate form of the text). To prevent hackers from accessing sensitive information, it should always be encrypted. Websites that communicate bank account and credit card information, for example, encrypt sensitive data to prevent fraud and identity theft.

B. Decryption

Decryption is the procedure of restoring data to its initial state, unencrypted state after encryption has rendered it unreadable. During decryption, the system extracts and turns the jumbled data into phrases and visuals that both the reader and the machine can understand. Decryption can be performed either manually or automatically. A set of keys or a password might also be used to carry it out.

II. METHODOLOGY/EXPERIMENTAL

A. User Interface Design and Platform Diversity

The methodology takes into account the diverse ways in which users access and interact with technology. It not only addresses the development of the graphical user interface (GUI) application but also recognizes the importance of extending these capabilities to a broader audience. Consequently, the approach encompasses the creation of a responsive website and a mobile application that share the same underlying principles for file encryption and decryption. The user interface design goes beyond aesthetics. It has been meticulously planned to accommodate the various screen sizes and input methods encountered in the digital landscape. This ensures that users can seamlessly transition between their desktop computers, laptops, smartphones, and tablets while enjoying a consistent and intuitive experience. Key design elements, such as button placement, color schemes, and typography, have been chosen to enhance accessibility and usability, catering to both tech-savvy users and those less familiar with encryption technology.

B. Encryption and Decryption Logic

At the heart of this methodology is a robust encryption and decryption logic that is implemented consistently across all platforms. This logic is designed to ensure both data security and ease of use.

The encryption process begins with the derivation of encryption keys from user-provided passwords and random salts. This step is fundamental to the security of the entire system. It employs a strong Key Derivation Function (KDF), such as PBKDF2, which iteratively transforms the password and salt into a secure encryption key.

To add an extra layer of security, the XOR (exclusive OR) operation is applied during encryption. This operation performs bitwise manipulation on the binary representations of the encrypted password and the file data. This ensures that even if one layer of encryption is compromised, the data remains highly secure.

Uniform encryption and decryption logic guarantee that users can expect a consistent level of security and functionality across the GUI application, website, and mobile app.

C. File Selection and Data Accessibility

The methodology recognizes that users' files are at the core of the encryption and decryption process. All three technologies have logical file selection and data accessibility processes built in to guarantee a smooth and effective workflow.

Users are empowered to select the files they wish to protect or access with ease. The process caters to the diverse needs of users who may be dealing with a wide range of file types, sizes, and sources.

By placing file selection front and center, the methodology prioritizes user control and convenience. This approach ensures that users can readily designate which files are to be encrypted or decrypted, giving them the flexibility to protect their most sensitive data.

D. Password Security and Privacy

Passwords play a pivotal role in the methodology. Recognizing their significance in securing data, this approach incorporates rigorous password security and privacy measures.

Password entry fields are thoughtfully designed to ensure the utmost confidentiality and privacy of sensitive information. The use of the show='●' attribute conceals characters as users type their passwords, mitigating the risk of prying eyes or potential keyloggers compromising security. Furthermore, password security extends to the backend, where robust cryptographic techniques are employed to transform passwords into encryption keys. This ensures that even if passwords are compromised, the encryption keys derived from them remain highly secure.

E. Encryption Process

The encryption process, which is a cornerstone of this methodology, offers users a straightforward and secure means to protect their files. It begins with the selection of target files, whether documents, images, or any other data. These selected files undergo encryption using the derived encryption keys. The methodology ensures that the encryption process is transparent to users, making data protection accessible to individuals with varying levels of technical expertise. Once encrypted, the files are securely stored, shielded from unauthorized access. The generation of complementary ".key" and ".salt" files is a critical part of the process. These auxiliary files, stored alongside the encrypted data, are vital for subsequent decryption operations.

F. Decryption Procedure

The decryption process mirrors the encryption procedure in its consistency and attention to security. Whether initiated on the GUI application, website, or mobile app, the same logic is applied.

The process commences with a systematic check for the presence of ".key" and ".salt" files that are associated with the target file. This verification ensures the integrity of the decryption process.

Subsequently, the methodology retrieves the saved password from the ".key" file, and, using the associated salt, derives the decryption key. This key is then applied to reverse the encryption process, restoring the files to their original state. This standardized decryption process prioritizes data recovery while maintaining robust security measures.

G. Security Measures and Consistency

Security is a foundational element of the methodology and is consistently emphasized across all platforms. To strengthen encryption keys, a Key Derivation Function (KDF) like PBKDF2 is used uniformly. KDF iteratively transforms user- provided passwords and salts into secure encryption keys, significantly enhancing their strength. Secure key management practices, such as the secure storage of keys and salts, are consistently enforced. These practices ensure that sensitive data remains confidential and is shielded from unauthorized access.

The methodology's commitment to security is unwavering, guaranteeing that users can trust the system to safeguard their most valuable data.

1) Platform Accessibility and User Guidance

A primary objective of this methodology is to provide accessibility to secure file encryption and decryption across various platforms. Recognizing the diversity of devices and preferences among users, the methodology ensures that the GUI application, website, and mobile app cater to a wide audience. In addition to platform diversity, the methodology places a strong emphasis on user guidance. Error messages and notifications are designed to be informative and helpful, ensuring that users are well-informed and capable of navigating the encryption and decryption processes with ease.

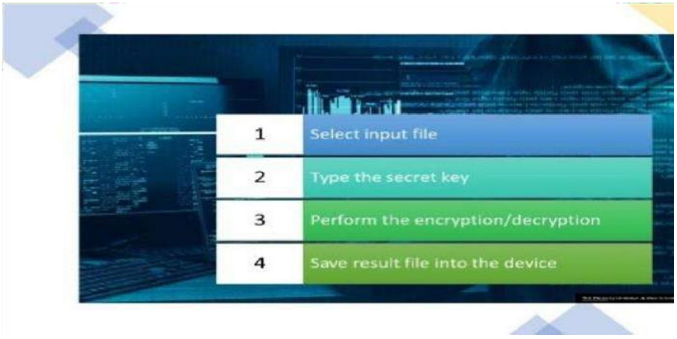


Fig 2: - Steps of Encrypting/Decrypting

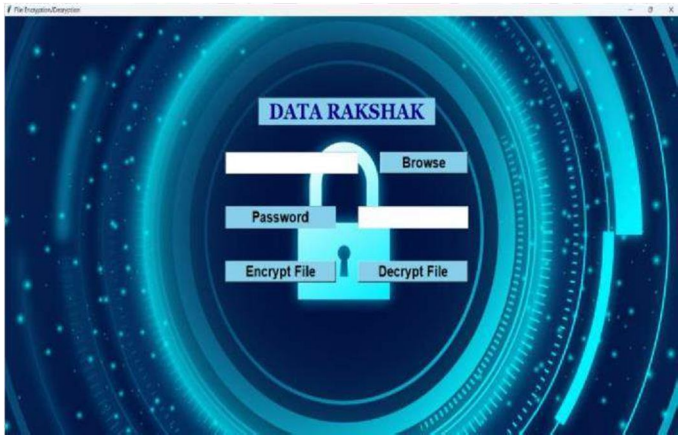


Fig 3: - GUI Interface

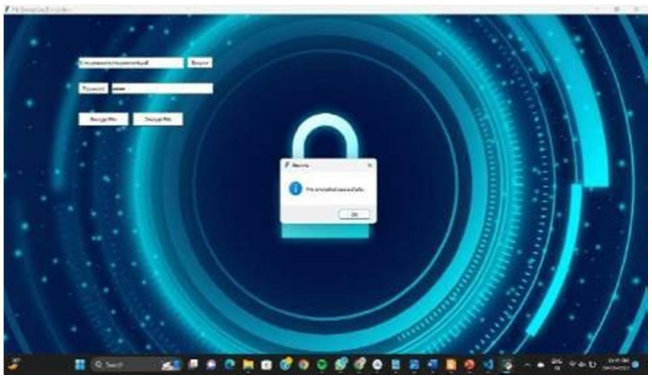


Fig 4: -File encrypted successfully.

Fig 5: - File decrypted successfully.

Fig 6:- Website Interface

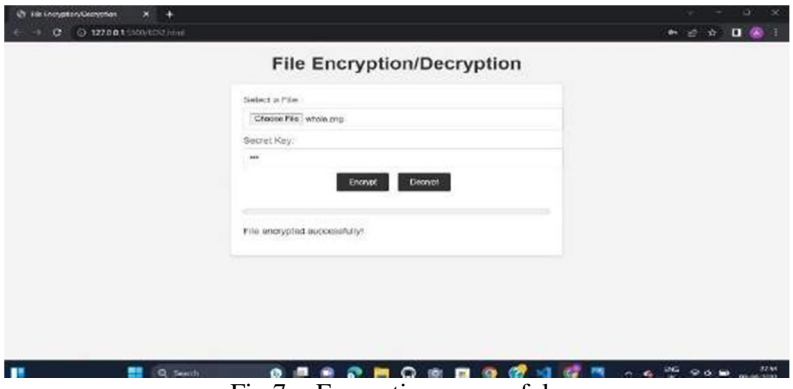


Fig 7 :- Encryption successful

Fig 8 :- App Interface

III. RESULTS AND DISCUSSIONS

Decryption is the process of restoring plaintext data from ciphertext, or incomprehensible data. The process of transforming plaintext, or readable information, into ciphertext, is known as encryption. Both encryption and decryption, which are the fundamental elements of cryptographic systems, guarantee the confidentiality and security of highly confidential data.

A secret key and an encryption method are used to encrypt the plaintext data. By rearranging the data according to the key, the algorithm creates the ciphertext. The ciphertext appears to be a random jumble of protagonists, making it difficult for those without authorization to decode the original transmission.

On the other hand, decryption includes using the opposite procedure. The ciphertext is decrypted using the same secret key and procedure, which then restores the original plaintext.

The recipient can successfully decipher the original message if they have the right decryption key.

It is important to keep in mind that both the difficulty of the algorithm and the privacy of the key have a significant impact on the robustness and security of encryption and decryption procedures. It is impossible for an attacker to decrypt the original message using strong encryption techniques.

The choice of encryption and decryption methods depends on the specific needs of the application, including the desired security level, the computational resources at hand, and the significance of the data that requires protection. As outlined in the subsequent sections, typical encryption methods encompass symmetric encryption, asymmetric encryption, and hybrid encryption.

IV. FUTURE SCOPE

After examining encryption algorithms, it has been determined that when key length increases, algorithm reliability likewise increases, but algorithm performance falls. We need to optimize the key length in order to get around this. Additionally, RSA was revealed to have vulnerabilities following analysis, and a new method has been proposed to fix these vulnerabilities. The suggested technique improves system security while also reducing time complexity. Work can be done in the future to make the algorithm less difficult.

There is a lot of space for expansion in an assortment of crucial areas, making the future of both decryption and encryption look promising. Here are some potential future directions:

1) *Post-Quantum Cryptography:* As quantum computers proliferate, it's possible that assaults on conventional encryption algorithms will become more common. Postquantum cryptography intends to provide encryption methods that can fend off assaults based on quantum computing, providing long-term security.
2) *Homomorphic Encryption:* Homomorphic encryption enables secure and privacy-preserving
3) *Blockchain and Cryptocurrency Security:* Strong encryption methods are required to protect transactions, digital wallets, and smart contracts as blockchain technology and cryptocurrencies advance. Future developments in encryption technology will be essential to boosting the security and reliability of blockchain-based systems.
4) *Quantum key distribution (QKD):* A method for securely transferring encryption keys between parties that makes use of quantum mechanics. It provides demonstrable protection from eavesdropping efforts. The secure key exchange in a variety of communication systems may be implemented with more QKD research and development
5) *Secure Internet of Things (IoT):* As the IoT ecosystem expands, it is critical to protect the confidentiality and security of data sent between IoT devices. Secure protocols and encryption methods designed for devices with limited resources will.

V. CONCLUSION

Encryption and decryption techniques stand as indispensable tools in the realm of cybersecurity and data protection. They play a pivotal role in preserving the confidentiality, integrity, and security of sensitive information, both in transit and at rest. These strategies employ sophisticated algorithms and cryptographic methods to transform plaintext data into unreadable ciphertext and then back into its original form, all while ensuring data remains secure from unauthorized access.

A. *The Role of Encryption*

Encryption serves as the cornerstone of modern digital security. Its primary objectives include:

1) *Confidentiality:* Encryption shields data from prying eyes. Even if an unauthorized party gains access to encrypted data, they will be unable to decipher it without the appropriate decryption key.
2) *Integrity:* Encryption ensures that data remains unaltered during transmission or storage. Any unauthorized modification to encrypted data becomes evident upon decryption.
3) *Authentication:* Cryptographic techniques, such as digital signatures, validate the authenticity of the sender and recipient, assuring that data has not been tampered with during transit.
4) *Symmetric and Asymmetric Encryption:* Encryption techniques are broadly categorized in two fundamental types: Symmetric Encryption and Asymmetric Encryption.
5) *Symmetric Encryption:* Symmetric encryption employs a secret key for encryption and decryption processes. This method is highly efficient and fast, making it well-suited for encrypting large volumes of data. However, the primary challenge in symmetric encryption lies in securely exchanging the secret key between parties.
6) *Asymmetric Encryption (Public Key Encryption):* Asymmetric encryption operates on a key pair, comprising a public key for encryption and a private key for decryption. This approach eliminates the need for a secure key exchange since the private key remains confidential. It is particularly advantageous for ensuring secure communication over untrusted networks.
7) *Data Integrity Verification:* To ensure data integrity, hash functions are employed to generate fixed-size hash values or checksums. These hash values act as digital fingerprints, allowing data recipients to verify that the data has not been tampered with during transmission.

B. *Hybrid Encryption:*

The benefits of symmetric and asymmetric encryption are combined in hybrid encryption.. It employs symmetric encryption to secure the data itself while using asymmetric encryption to protect the symmetric key during key exchange. This approach provides both efficiency and security, addressing the challenges of secure key distribution.

C. *Transport Layer Security (TLS)*

TLS is a critical protocol for ensuring secure network connections. It encrypts data during transit, safeguarding against eavesdropping and data tampering. TLS relies on asymmetric encryption for key exchange and symmetric encryption for efficient data transmission. In the rapidly evolving digital landscape, encryption and decryption techniques are the linchpin of data security.

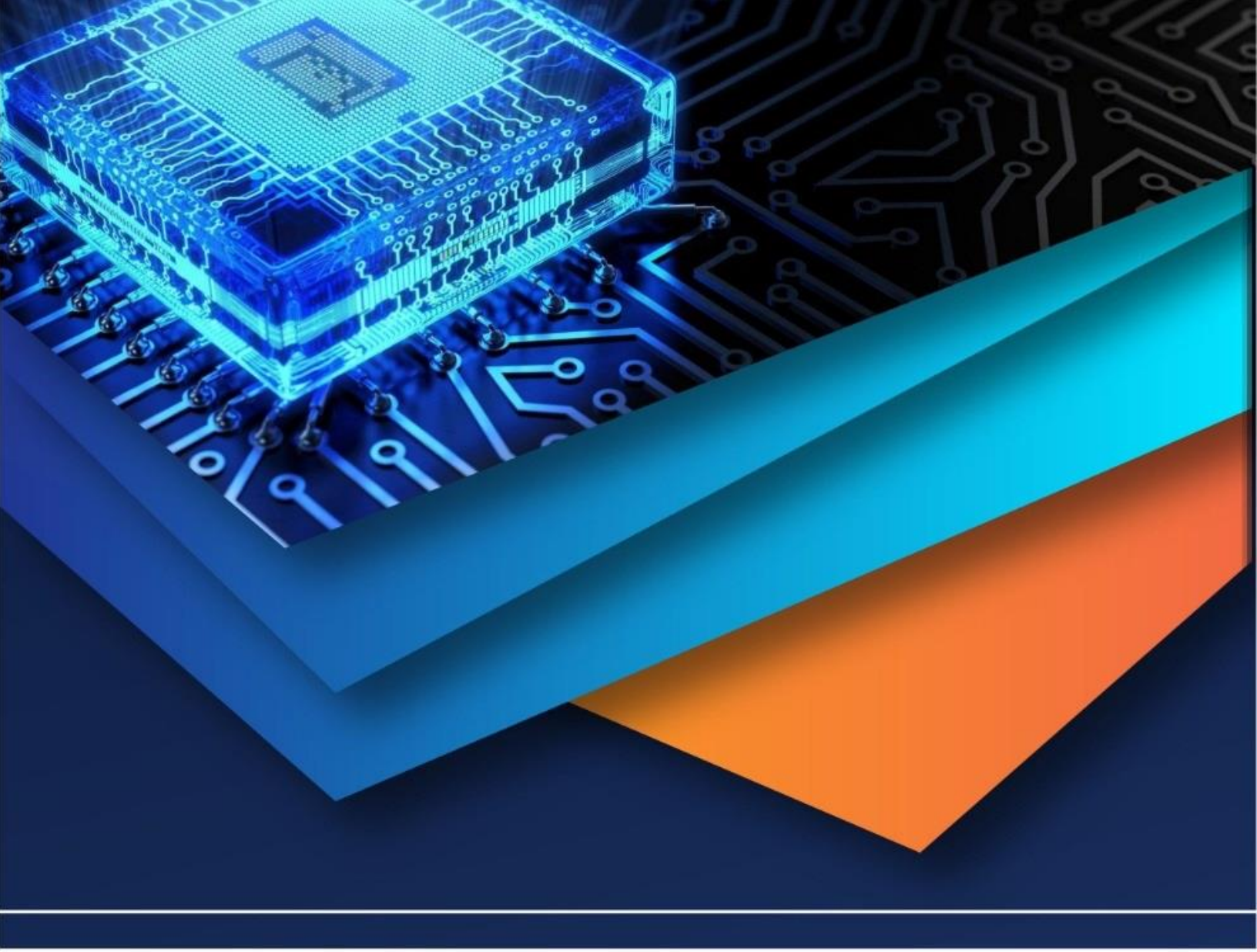
Whether used in secure communication channels, data storage, or authentication processes, these techniques are vital for safeguarding sensitive information from the prying eyes of cyber threats. As technology advances, encryption methods continue to adapt and strengthen, providing a robust defense against evolving security challenges.

REFERENCES

[1] Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing.
[2] arXiv preprint arXiv:1101.5613 Rahmati, Qian, & Zhong. (2007).
[3] Understanding human-battery interaction on mobile phones. Proceedings of the 9th international conference on Human-computer interaction with mobile devices and services, 265-272. doi:10.5121/ijnsa.2011.3103 Dawood, A. (2019).
[4] An adaptive intelligent alarm system for wireless sensor network. Indonesian Journal of Electrical Engineering and Computer Science, 15(1), 142– 147.
[5] doi:10.11591/ijeecs. v15.i1. pp142-147 Saini, B. (2014).
[6] Survey on Performance Analysis of Various Cryptographic Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 4, 1–4. Subramanyan, B., Chhabria, V.M., & Babu, T. S. (2011).
[7] Image encryption based on AES key expansion. 2011 Second International Conference on Emerging Applications of Information Technology, 217-220.
[8] doi:10.1109/ EAIT.2011.60 Krintz, C., Wen, Y., & Wolski, R. (2004). Application-level prediction of battery dissipation. Proceedings of the 2004 international symposium on Low power electronics and design, 224-229.

doi:10.1145/1013235.1013292 Li, C., Lin, D., & Lü, J. (2017).

9. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE MultiMedia, 24(3), 64– 71. doi:10.1109/MMUL.2017.3051512 Elminaam, D. A., Kader, H. A., & Hadhoud, M. M. (2009). Performance evaluation of symmetric encryption algorithms. Communications of the IBIMA, 8, 58–
64. Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab,
H. A., Shabbir, M., & Al-Nabhani, Y. (2010).
10. New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085. Cheng, H., & Lerner, C. (2015).
11. Bit allocation for lossy image set compression. Communications, Computers and Signal Processing (PACRIM), 2015 IEEE Pacific Rim Conference on, 52- 57. doi:10.1109/PACRIM.2015.7334808
Hussain, I., Shah, T., & Mahmood, H. (2010).
12. A new algorithm to construct secure keys for AES. International Journal of Contemporary Mathematical Sciences, 5, 1263–1270. Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish:
13. Symmetric key cryptography algorithms simulationbased performance analysis. International Journal of Emerging Technology and Advanced Engineering, 1, 6–12. Korhonen. (2011).
14. Predicting mobile device battery life. Department of Communication and Networking, S-38. Khalaf, O. I., & Abdulsahib, G. M. (2019).
15. Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network. Journal of Information Science and Engineering, 35(5), 1099–1112.
16. Khalaf, O. I., & Sabbar, B. M. (2019).
17. An overview on wireless sensor networks and finding optimal location of nodes. Periodicals of Engineering and Natural Sciences, 7(3), 1096–1101. doi:10.21533/pen. v7i3.645 Khalaf, O. I. (2020). Optimization of wireless sensor network coverage using the Bee Algorithm. Journal of Information Science and Engineering, 36(2), 377–386.
18. Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., & Ogudo, K. A. (2020). A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY