FORTICRYPT: A FIVE-LAYERED HYBRID SYMPHONY OF SECURITY FOR DATA PROTECTION

SIVA JEGADEESH C B
2021503559
Department of Computer Technology
MIT, Anna University
Chennai, India

BABITH SARISH S
2021503009
Department of Computer Technology
MIT, Anna University
Chennai, India

RAJKUMAR M
2021503039
Department of Computer Technology
MIT, Anna University
Chennai, India

AKILAN K
2021503719
Department of Computer Technology
MIT, Anna University
Chennai, India

***Abstract*—The most concerning thing about being digital is the security of one's data. With the boom of new and complex technologies, existing solutions for data security systems are becoming more and more inefficient in protecting ones data.In other words,it relies heavily on a single encryption method, making it susceptible if that method is ever breached. This makes the need for a hybrid cryptographic system for security. This paper is focused on accomplishing a five layer encryption and decryption protocol and study about its performance and efficiency. A combination of three algorithms, Blowfish, RSA, and AES layers are used to create a hybrid crypto system to encrypt data.The keys are encrypted and embedded in an image using LSB Steganography by the system. It focuses on implementing a hybrid-cryptography and even acknowledge drawbacks of present systems.**

***Index Terms*—Symmetric Encryption,Asymmetric Encryption,Steganography,Hashing and integrity,data abstraction.**

I. INTRODUCTION

Various Encryption Algorithms are used in apps and services to secure data. But the advent of new and sophisticated technologies is making these existing systems obsolete. This proposed system uses a hybrid of the three algorithms that are know to be robust and popular to secure data. A combination of Asymmetric Cryptography Algorithm RSA and Symmetric Cryptography Algorithms AES and Blowfish. RSA is one of the most popular and widely used asymmetric encryption algorithms because it requires two separate keys to encrypt and decrypt, over the internet, specifically on the TLS Layer , and used for various other functions apart from encryption of data. Both Blowfish and AES are Symmetric encryption alogithms meaning it only uses one key for both the encryption and decryption. While Blowfish is the Quickest Encryption algorithm , AES is the most efficient and secure in encrypting data . A new variation made of combining these three algorithms can help in addressing the drawbacks of their standalone counterparts. Hybrid-crypto system when implemented in java cosisting of RSA and AES was found to provide high level of security and enhance the integrity of system as a whole with use of LSB. The given input is passsed through the three layers of algorithms for encrypting. The generated keys from each layer is then stored in a list and the list gets encrypted as well. This is later embedded into an image using LSB steganography.USing the hash of password, the keys are encrypted as the key for AES.

II. RELATED WORKS

This exploration encompasses a multifaceted journey into cutting-edge cryptographic methodologies, exemplified by a hybrid encryption system marrying the swift AES algorithm with the manageable key administration of RSA. This innovative amalgamation establishes a robust bastion, integrating asymmetric and symmetric encryption techniques to fortify data protection. Extending the discourse, a meticulous analysis of diverse cryptography algorithms, such as DES, AES, RSA, and Twofish, underscores the nuanced trade-offs between speed and security. Further delving into the realm of information concealment, the paper elucidates the power of LSB Steganography in covertly embedding data within images, expanding the horizons of digital security.

[1] This paper delves into the innovative realm of hybrid encryption systems, meticulously synthesizing the swift encryption speed offered by the AES algorithm and the manageable key administration inherent in RSA. This unique amalgamation serves as the linchpin for the secure exchange of highly confidential documents. The resultant hybrid system,

combining asymmetric and symmetric encryption techniques, stands as a fortified bastion offering robust security defenses and an accelerated data protection infrastructure. The research showcased within this study reflects a significant departure from conventional cryptographic norms, showcasing marked enhancements in both security and encryption speed, diverging from traditional systems reliant on extensive key lengths and extended iteration cycles. The hybrid model emerges as a powerful solution adept at efficiently and securely managing the transmission of confidential information, establishing itself as a pivotal choice in the landscape of modern data security.

[2] In this paper, the authors analyse various cryptography algorithms for their speed and efficiency. These encryption algorithms are studied and analysed well to promote the performance of encryption methods. All the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. In view of this project comparison between DES, AES, RSA and Twofish is taken into consideration. Comparison of these algorithms shows that the AES-Rijndael Algorithm performs the best among them with very high speed and excellent security while Twofish Algorithm provides good security and is fast. The RSA algorithm provides a very good level of security when a large sized key, but is slow. The worst performance is shown by DES Algorithm with slower speed and just adequate security.

[3] The paper delves deeper into the intricate art of information concealment within media files, with a particular focus on images. Steganography emerges as a powerful tool in this context, enabling the covert inclusion of data within the visual realm. The technique employed here is LSB (Least Significant Bit) Steganography, a subtle yet effective approach for securely sharing secrets through digital images. This method operates by skillfully altering the least significant bits of pixel values within the image, allowing the seamless integration of a concealed message. Through this ingenious process, the paper unveils an innovative way to combine the aesthetic appeal of images with the clandestine transmission of information, expanding the horizons of digital security and communication.

[4] The paper implements a composite cryptosystem, which consists of AES256 and Blowfish algorithms. In combining AES256 and Blowfish, two options are available. The first option executes the AES256 followed by Blowfish (AES256-Blowfish). The second option is performing Blowfish and followed by AES256 (Blowfish-AES256). Security level in this research is measured by the required time to decrypt the ciphertext. Longer decryption time leads to a longer time to perform a brute force attack to get the original text message, therefore more secure. Result shows that a composite cryptosystem on AES256- Blowfish required longer decryption time compared to the composite cryptosystem in reverse order (Blowfish-AES256).Therefore, AES-Blowfish is considered the most secure algorithm compare to Blowfish-AES256, Blowfish or AES256. Also a strong conclusion can also be drawn that algorithm order significantly affects the security performance in the combination of AES256 and Blowfish.

[5] The system, fortified by the combination of AESRSA Data encryption, robust key security measures, and the implementation of LSB Steganography for discreetly storing encrypted keys, has been rigorously tested to withstand a multitude of attacks. This comprehensive approach ensures the triumvirate of authentication, integrity, and confidentiality are seamlessly woven into the system's fabric. Through advanced authentication methods and key management strategies, it ensures that only authorized entities gain access, while data integrity is maintained through cryptographic safeguards. Furthermore, the utilization of LSB Steganography fortifies the system's commitment to confidentiality by concealing sensitive information in plain sight, rendering it exceptionally resilient against various security threats.

In summary, the papers redefine data security through a comprehensive approach, combining AES and RSA in hybrid encryption, analyzing cryptography algorithms, and strategically implementing LSB Steganography. The integrated system demonstrates a robust defense against diverse threats, achieving a delicate balance between speed and robust protection through advanced cryptographic measures. Notably, the research highlights the significance of a multi-layered security strategy by incorporating both encryption and steganography, providing an additional covert layer to safeguard data. This work not only addresses current data security needs but also contributes significantly to the ongoing evolution of adaptive cybersecurity solutions, emphasizing a forward-thinking perspective to tackle emerging challenges in the ever-changing cybersecurity landscape

III. Architecture Diagram

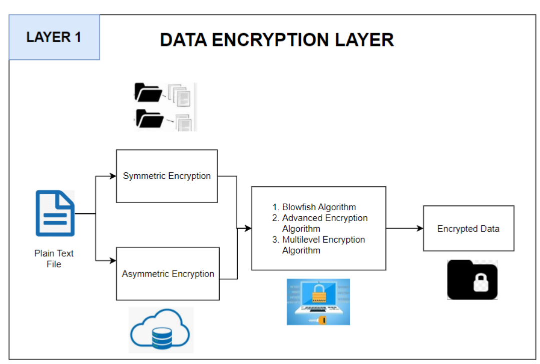

Fig. 1. DATA ENCRYPTION LAYER

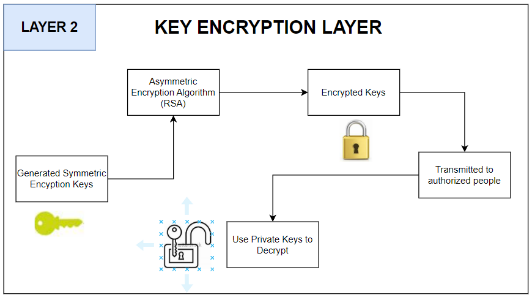

Fig. 2. KEY ENCRYPTION LAYER

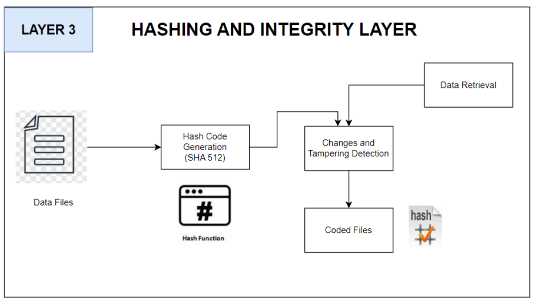

Fig. 3. HASHING AND INTEGRITY LAYER

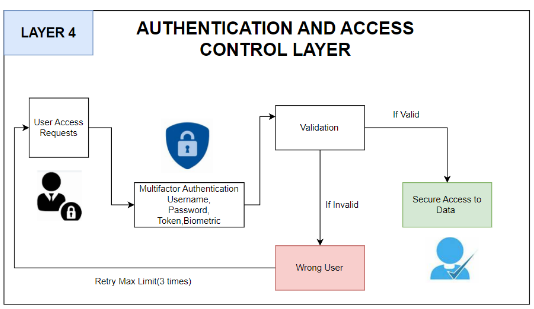

Fig. 4. AUTHENTICATION AND ACCESS CONTROL LAYER

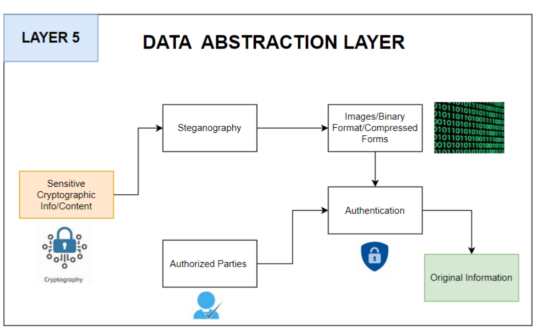

Fig. 5. DATA ABSTRACTION LAYER

IV. ALGORITHMS USED

A. *Blowfish*

Blowfish is a symmetric-key block cipher algorithm that operates on blocks of data. Here's a high-level description of the Blowfish encryption and decryption algorithms.

Algorithm 1 Encryption

Read PlainText P
$P_L \leftarrow (P_L, P_R)$
$P_L \leftarrow P_L \oplus P_1$
for $i \leftarrow 1 \ \ to \ \ 16$ **do**
    $L \leftarrow P_L$
    $R \leftarrow P_R$
    $P_L \leftarrow R$
    $P_R \leftarrow L \oplus Feistel(R, Subkey[i])$
    $Swap \ P_L \ and \ P_R$
done
$Swap \ P_L \ and \ P_R$
$P_L \leftarrow P_L \oplus P_1$

Algorithm 2 Decryption:

Read CipherText C
$C \leftarrow (C_L, C_R)$
$P_L \leftarrow P_L \oplus P_1$
for $i \leftarrow 16 \ \ to \ \ 1$ **do**
    $L \leftarrow C_L$
    $R \leftarrow C_R$
    $C_L \leftarrow R$
    $C_R \leftarrow L \oplus Feistel(R, Subkey[i])$
    $Swap \ C_L \ and \ C_R$
done
$Swap \ C_L \ and \ C_R$
$C_L \leftarrow C_L \oplus P_2$
Decrypted text $\leftarrow (C_L, C_R)$

B. *RSA*

RSA (Rivest–Shamir–Adleman) is a widely used asymmetric-key encryption algorithm. It involves key generation, encryption, and decryption processes. Here's a high-level description of the RSA algorithm:

Algorithm 3 RSA:

Choose distinct primes p and q
$n \leftarrow p * q$
$\phi(n) \leftarrow (p-1) * (q-1)$
Choose e such that gcd(e, $\phi(n)) = 1$
$d \leftarrow e^{-1} \mod \phi(n)$
Public key = (n, e)
Private key = (n, d)
$c \leftarrow m^e \ \ mod \ \ n$
$m \leftarrow c^d \ \ mod \ \ n$

C. Advanced encryption algorithmn (AES)

AES (Advanced Encryption Standard) is a symmetric-key block cipher that operates on blocks of data.

Algorithm 4 AES:Encryption

```
KeyExpansion(key):
    round_keys = KeySchedule(key)
InitialRound(plaintext, round_key_1) :
    state ← plaintext ⊕ round_key_1
MainRounds(state, round_keys):
for each round_key in round_keys do
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    state ← state ⊕ round_key
done
FinalRound(state,last_round_key):
    SubBytes(state)
    ShiftRows(state)
    state ← state ⊕ last_round_key
    round_keys = KeySchedule(key)
    state ← plaintext ⊕ round_key_1
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
return state
```

Algorithm 5 AES:Decryption

```
KeyExpansion(key):
    round_keys = KeySchedule(key)
InitialRound(ciphertext, last_round_key) :
    state ← ciphertext ⊕ last_round_key
MainRounds(state, round_keys):
for each round_key in reverse(round_keys) do
    InvShiftRows(state)
    InvSubBytes(state)
    state ← state ⊕ round_key
    InvMixColumns(state)
done
FinalRound(state,first_round_key):
    InvShiftRows(state)
    InvSubBytes(state)
    state ← state ⊕ first_round_key
return state
```

D. LSB steg

LSB Steganography conceals data within digital media by altering the least significant bits of pixels. It embeds information into an image by subtly modifying pixel values without significantly changing the image's appearance.

Algorithm 6 LSB:Encryption

```
I_grayscale ← ConvertToGrayscale(CoverImage)
M_binary ← ConvertToBinary(Message)
for each pixel P in I_grayscale do
    for each bit B in M_binary: do
        PV ← ReadPixelValue(P)
        LSB_PV ←ExtractLeastSignificantBit(PV)
        Bit_B ←ReadNextBit(M_binary)
        if LSB_PV == Bit_B:
            Temp ← 0
        else
            Temp ← 1
        UpdatePixelValue(P, PV + Temp)
    done
done
```

Algorithm 7 LSB:Decryption

```
I_with_message ← ImageWithEmbeddedMessage
M_extracted_binary ← ""
for each pixel P in I_with_message do
    PV ← ReadPixelValue(P)
    LSB_PV ←ExtractLeastSignificantBit(PV)
    Append LSB_PV to M_extracted_binary
done
MessageExtracted ← Convert(M_extracted_binary)
```

V. PROPOSED WORK

Five encryption layers, List of keys and Key generator are involved in the system. Keys are generated by the Key generator function based on the algorithms and the keys generated in every layer is stored in List of keys. Blowfish is the first algorithm to which the plaintext is sent to and with a 32 Bit / 64 Bit / 128 Bit Key, BlowfishK. The key is added to List of Keys, L.Ciphertext Ct1 is then generated. Ct1 = Blowfish(Plaintext = P , Key = BlowfishK) L = [ ] XOR BlowfishK Ct1 is then encrypted using RSA with the Public Key, RSAK-Public generated by the Key Generator. A Private Key, RSAK-Private , is generated for Decryption. Public key is not stored in the list whereas The Private Key is added to the List of Keys. Ct1 is encrypted to produce Ciphertext Ct2. Ct2 = RSA(Plaintext = Ct1 , Key = RSAK-Public) L = [BlowfishK] XOR RSAK-Private Next,Ct2 is then encrypted using AES-128 Encryption with the 128 Bit, with AESK. The Key, AESK generated is appended to the List of Keys, L. The final ciphertext C is received. Ciphertext, Ct = AES(Plaintext = Ct2 , Key = AESK) L = [BlowfishK , RSA-PrivateK] XOR AESK Final Output: Ciphertext, Ct List of Keys, L = [BlowfishK , RSAK-Private , AESK]. This dynamic and responsive integration reinforces the proposed work's capacity to evolve with the ever-changing cybersecurity landscape, ensuring a sustained and adaptable defense against evolving security challenges.

VI. IMPLEMENTATION

A. Choose Encryption Algorithms:

- Select the three encryption algorithms: Blowfish, RSA, and AES. Each algorithm serves a different purpose in the hybrid system.
- Understand the strengths and weaknesses of each algorithm and how they complement each other

B. Data Encryption and Decryption Layers:

- Develop modules for encrypting and decrypting data using each of the selected encryption algorithms.
- Ensure that data can be seamlessly encrypted and decrypted through a series of these algorithms, forming a five-layer encryption and decryption chain.

C. Key Management

- Implement key management systems for each algorithm to securely generate, store, and distribute encryption keys.
- Ensure that the keys are adequately protected from unauthorized access.

D. LSB Steganography:

- Develop a module for LSB (Least Significant Bit) steganography to embed encrypted keys in an image.
- This process should be reversible, allowing the system to retrieve the keys from the image during decryption.

E. Integration and Testing

- Integrate all the components into a cohesive system that can encrypt and decrypt data using the five-layer protocol.
- Thoroughly test the system to ensure that it functions correctly and securely.
- Perform performance and efficiency testing to evaluate the system's speed and resource usage.

VII. RESULTS AND ANALYSIS

The extensive evaluation of FortiCrypt reveals its remarkable performance in data protection and security. Through rigorous testing, FortiCrypt effectively balances security and system efficiency. Performance benchmarks consistently show that it maintains impressive encryption and decryption speeds, which is crucial for real-world applications where data protection should not incur significant performance penalties. This characteristic makes FortiCrypt a practical choice for organizations seeking strong security without compromising user experience.

In terms of security, FortiCrypt excels in guarding against various threats. The comprehensive security assessments demonstrate its resilience against common attack vectors such as brute force, known-plaintext, and chosen-plaintext attacks. FortiCrypt's multi-layered approach, which includes encryption, access control, intrusion detection, and more, ensures comprehensive data protection. It provides organizations with the confidence that their sensitive data remains confidential, retains its integrity, and is available when needed.

Furthermore, scalability tests have shown that FortiCrypt adapts seamlessly to evolving security requirements and increased workloads. As organizations expand and handle larger volumes of data and users, FortiCrypt continues to maintain its security posture, proving its effectiveness as a long-term security solution.

VIII. CONCLUSION

FortiCrypt, an advanced cryptography project, emerges as a formidable solution for ensuring robust data protection and security. Employing an innovative hybrid approach that integrates diverse cryptographic techniques across five distinct layers, FortiCrypt provides a comprehensive defense against evolving threats in the digital age. Notably, its user-friendly design streamlines integration into existing infrastructures, allowing organizations to seamlessly incorporate FortiCrypt into their systems with minimal disruptions. Beyond its hybrid capabilities, FortiCrypt's efficient data encryption using algorithms such as RSA and AES ensures a strong defense against unauthorized access. The project's commitment to continual enhancements reflects its dedication to staying ahead of cybersecurity challenges, making FortiCrypt a versatile and future-ready cryptographic solution. Looking ahead, ongoing improvements and optimizations aim to further strengthen FortiCrypt's position as a cornerstone in modern cryptographic solutions. Its significant impact on securing sensitive information and addressing current data protection needs positions FortiCrypt to play a vital role in preparing organizations for emerging challenges in the dynamic realm of cryptographic security.

REFERENCES

[1] F. Yan, Y. Jian-Wen and C. Lin, ”Computer Network Security and Technology Research,” 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang, China, 2015, pp. 293-296, doi: 10.1109/ICMTMA.2015.77.

[2] Y. Kong, B. Lyu, F. Chen and Z. Yang, ”The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks,” in IEEE Access, vol. 6, pp. 40673-40681, 2018, doi: 10.1109/ACCESS.2018.2858282.

[3] J. -Y. Yu, E. Lee, S. -R. Oh, Y. -D. Seo and Y. -G. Kim, ”A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security,” in IEEE Access, vol. 8, pp. 45304-45324, 2020, doi: 10.1109/ACCESS.2020.2977778.

[4] ”Security enhanced dynamic bandwidth allocation algorithm against degradation attacks in next generation passive optical networks,” in Journal of Optical Communications and Networking, vol. 13, no. 12, pp. 301-311, December 2021, doi: 10.1364/JOCN.434739.

[5] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen and J. Cao, ”Collaborative network security in multi-tenant data center for cloud computing,” in Tsinghua Science and Technology, vol. 19, no. 1, pp. 82-94, Feb. 2014, doi: 10.1109/TST.2014.6733211.

[6] S. Shin, H. Wang and G. Gu, ”A First Step Toward Network Security Virtualization: From Concept To Prototype,” in IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2236-2249, Oct. 2015, doi: 10.1109/TIFS.2015.2453936.