The Development of Hybrid Technique for Encryption Application

Ahmad Luqman Bin Ahmad Kamal Ariffin
Faculty of Information Sciences & Engineering
Management & Science University
Shah Alam, Malaysia
ahmad_luqman@msu.edu.my

Kishan Vasuthevan
Faculty of Information Sciences & Engineering
Management and Science University
Shah Alam Malaysia
kvasuthevan7@gmail.com

2024 IEEE 12th Conference on Systems, Process & Control (ICSPC) | 979-8-3503-9139-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSPC63060.2024.10861952

***Abstract*— This study introduces an innovative hybrid data encryption technique to enhance data confidentiality by integrating Rivest-Shamir-Adleman (RSA) encryption with dynamic key generation. The problem addressed is the vulnerability of traditional encryption methods to evolving cyber threats, which compromise both security and computational efficiency. To mitigate these risks, the proposed hybrid approach combines RSA's asymmetric encryption with dynamic key generation, using RSA primarily for generating encryption keys. This method enhances data security by frequently changing keys, reducing the risk of key compromise. Additionally, mechanisms for app-to-app data transfer integrity and authentication ensure data remains secure and unaltered throughout the communication process. The focus of this research is the development of a robust encryption system that transforms plaintext into ciphertext, providing a reliable means of protecting sensitive information across a range of applications. Results demonstrate the hybrid approach's resilience to various cyber threats while optimizing computational resources. In conclusion, the study aims to strengthen modern encryption systems by incorporating robust cryptographic algorithms with dynamic key generation, providing enhanced protection against emerging security challenges.**

Keywords*— *hybrid data encryption technique, data confidentiality, Rivest-Shamir-Adleman (RSA) encryption, dynamic key generation, cyber threats, security, computational efficiency, asymmetric encryption, data security, encryption keys, app-to-app data transfer integrity, authentication, robust encryption system, plaintext, ciphertext, sensitive information, cryptographic algorithms.

I. INTRODUCTION (*HEADING 1*)

Securing sensitive information has become a critical aspect of our lives. With the increasing number of cyber threats and data breaches, there is a growing need for hybrid data encryption techniques to ensure the confidentiality, integrity, and authenticity of data. One of the recent data breaches in Malaysia occurred in 2020, where personal data of millions of Malaysian citizens was leaked online. According to the article, the data breach involved the personal data of over 46 million Malaysian mobile phone users, including their names, phone numbers, and IC numbers. The data was reportedly leaked on a hacking forum, and it was not clear how the data was obtained or who was responsible for the breach. The Malaysian Communications and Multimedia Commission (MCMC) confirmed the incident and advised the public to be cautious about phishing scams and identity theft. This incident highlights the importance of data privacy and the need for organizations to implement strong security measures to protect personal data [1].

While traditional encryption methods such as symmetric and asymmetric encryption have been around for a long time, they face challenges such as high computational costs and vulnerability to attacks. Adopting innovative approaches to address these issues is critical. Hybrid techniques, which combine different methodologies, provide a solution for improving cryptographic algorithm security. This study assesses the efficacy of hybrid approaches, specifically integrating dependable RSA encryption with dynamic key generation, with the goal of providing a competent and adaptable solution in the ever-changing landscape of information security[2]. To ensure data security, the proposed hybrid data encryption approach combines dynamic algorithm key encryption and RSA asymmetric encryption. The system becomes a leading option for secure communication and secret data storage in modern applications by leveraging RSA for dynamic algorithm key generation [3].

This is a significant project that focuses on creating a more robust, efficient, and scalable hybrid encryption technique to improve the security of sensitive data across multiple devices. The goal of analyzing existing techniques is to overcome limitations, providing improved security and efficiency, with implementation and testing using diverse datasets to evaluate the effectiveness and security of the proposed technique.

Lack of security in existing encryption technologies is a major challenge. Traditional data transmission methods, which are widely used, can sometimes fall short of preventing complex attacks. With the rapid expansion of the Internet and increased mobile device usage, strong communication security is more important than ever. The reliance on a single key for both encryption and decryption in classical encryption, known as symmetric key encryption, is a fundamental flaw. It is critical to securely transmit this key between sender and receiver. otherwise, attackers could quickly decrypt the data. Furthermore, if the key is lost or stolen, all encrypted data is rendered insecure [8].

Third-party data breaches, specifically those resulting from cross-platform file exchanges, have arisen as a pressing concern in the field of data security. The exchange of encrypted file across platforms introduces vulnerabilities that criminals may misuse, resulting in unauthorized access and potentially sensitive information compromise. For example, In January 2020, hackers abused a third-party application that Marriott used to provide guest services. The assailants successfully obtained unauthorized entry to 5.2 million records including information about Marriott guests. The

records contained passport data, contact information, gender, birthdays, loyalty account details, and personal preferences (dmytro.tkach@apriorit.com, 2023).

When the encrypted message may be readily transformed into the original message, it presents substantial security vulnerabilities by compromising the secrecy of important data. This vulnerability enables malicious individuals to exploit weaknesses in encryption systems, potentially leading to unauthorized entry, data breaches, and the compromising of confidential information. This situation not only reduces personal privacy, but also presents risks to the security of organizations and society as a whole, highlighting the urgent requirement for robust encryption techniques to safeguard the integrity of information and prevent adverse outcomes.

The objectives of this research are geared toward advancing the security and privacy of hybrid data encryption systems in modern digital communications. Firstly, the study aims to fortify these systems by incorporating robust cryptographic algorithms alongside dynamic key generation techniques, ensuring enhanced protection against emerging threats. Secondly, it seeks to improve transmission security by implementing mechanisms for app-to-app data transfer integrity and authentication, which will guarantee that data remains secure and unaltered throughout the communication process. Lastly, the research focuses on the development of a robust encryption system that utilizes asymmetric encryption techniques to effectively transform plaintext into ciphertext, providing a secure and reliable method for safeguarding sensitive information across diverse applications.

II. LITERATURE REVIEW

A. Review of Current Situation

This literature review highlights the significance of data encryption for ensuring security and presents the concept of hybrid encryption, which integrates both symmetric (such as AES) and asymmetric (such as RSA) encryption techniques. AES is renowned for its robust security and optimal efficiency, frequently employed as a fundamental component in hybrid encryption systems. Hybrid encryption seeks to achieve a balance between security and efficiency by utilising the advantages of both encryption methods. Symmetric encryption, such as AES, is highly efficient but encounters difficulties in ensuring secure key distribution [4]. Asymmetric encryption, like RSA, deals with the issue of distributing keys, but it is characterised by slower speed and more resource consumption. The objective of this encryption synthesis is to enhance security in the process of transmitting and storing data.

B. Review of Related Literature

Current Situation of a New Hybrid Technique for Data Encryption In recent years, efforts have been made to enhance data security while minimizing computational overhead in encryption methods. Various strategies have been explored, such as using ASCII values in symmetric key encryption and bitwise operators in C programming to generate Pseudo-Noise Sequences, aiming to reduce energy consumption in communication [5]. New encryption calculations involving staggered information encryption, Fibonacci number generation for plaintext-to- ciphertext conversion, Unicode symbol conversion, FFT- based text file encryption, block-wise encryption, rotation, logical XOR operations, and one-time subkey derivation have been proposed.

Secure Electronic Transactions employ multiple encryption techniques to protect data confidentiality and prevent unauthorized access to wireless networks. Recent efforts focus on combining cryptography and steganography to prevent digital data tampering [6]. Additionally, there have been investigations into using Fibonacci representations for secure transmission of unbounded strings. Overall, advancements in encryption methods aim to enhance data security, minimize computational overhead, prevent unauthorized access, and safeguard digital information against tampering or manipulation.

Table 1: Comparison Table

AxCrypt, BitLocker, VeraCrypt, and HtCrypt are encryption programmes that each have their own set of features. BitLocker is a Windows tool that provides full disc encryption. VeraCrypt is an open-source alternative that supports a variety of encryption algorithms and operating systems. Whereas, AxCrypt is user-friendly and focuses on file-level encryption. HtCrypt has an extensive list of features, including strong encryption, secure file sharing, and an easy-to-use interface. When compared to other encryption tools, its focus on user experience differentiates it, making it suitable for users of all levels.

III. RESEARCH METHODOLOGY

The design and methodology of research encompass the comprehensive strategy and approach employed to carry out a research project and gather relevant data. It entails selecting the most appropriate methodologies, protocols, and tools to fulfil research goals and respond to research inquiries. This pivotal stage establishes the methodology for data collection, analysis, and interpretation. The research design and methodology establish a framework to ensure the study's findings are valid, reliable, and applicable by using a systematic and structured approach.

A. Development Methodology

The agile methodology is a method for developing software that is adaptable and iterative and focuses on producing high-quality products through collaboration and ongoing improvement. The following steps in Figure 1 were taken to develop a hybrid data encryption application using the agile methodology.

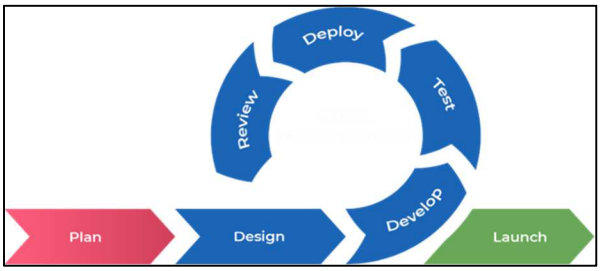

Figure 1: Agile Development Methodology

The first step, is to determine the application's goals, requirements, and scope for the hybrid data encryption techniques. making an item overabundance, which is a focused-on rundown of highlights and errands.

Second step, is to identify the key management, encryption algorithms, and other technical aspects necessary for the hybrid technique.

Third step, is the development stage which includes composing the code for the application. Isolating the work into little, reasonable errands called client stories. Each user story is a representation of a particular feature or function.

Fourth step, testing is a necessary piece of the light-footed approach. executing a variety of tests, including system testing, integration testing, and unit testing, to guarantee that the application works as intended and satisfies the specifications.

Fifth step, is deploying the application into a staging or production environment following completion of the development and testing phases. Guarantee that the application is appropriately introduced and arranged, prepared for use.

Sixth step, is conducting a review to evaluate the hybrid technique for data encryption application's overall progress and quality after deployment. evaluate the features that have been implemented, look for any problems or enhancements, and get feedback from stakeholders.

Final step, is to proceed with the application's official launch once the review phase is finished and any necessary adjustments have been made. Ensure that it is accessible to the intended users and communicate any necessary documentation or instructions.

B. Class Diagram and Use Case Diagram

Figure 2 illustrates how the system works. It starts with a Registration of account using a registered email address, followed by managing passwords, logging user activity, and allowing the user to log in and log out. Users will then have a user id and can set up their account. Then, encryption and decryption, which enable users to encrypt and decrypt data using the hybrid encryption technique. This involves selecting the appropriate encryption method and key for the data being encrypted or decrypted, and executing the encryption or decryption process. Finally, the data transfer, it allows users to seamlessly exchange encrypted files. Senders use the recipient's user ID to transmit encrypted files, while recipients utilize a private key to decrypt and view the incoming files. Similarly, users sending encrypted files can view both the encrypted and decrypted versions in the incoming scope, ensuring a secure and transparent data transfer process. Figure 3 shows a use case diagram for encrypt file that allows users to select file, generate, securing key exchange and decrypt file.

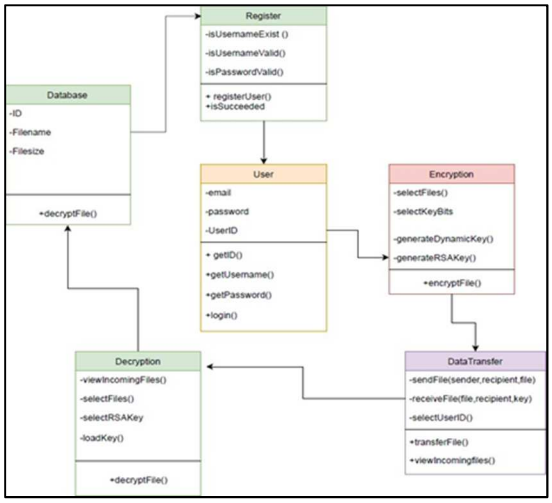

Figure 2: Class Diagram of HtCrypt

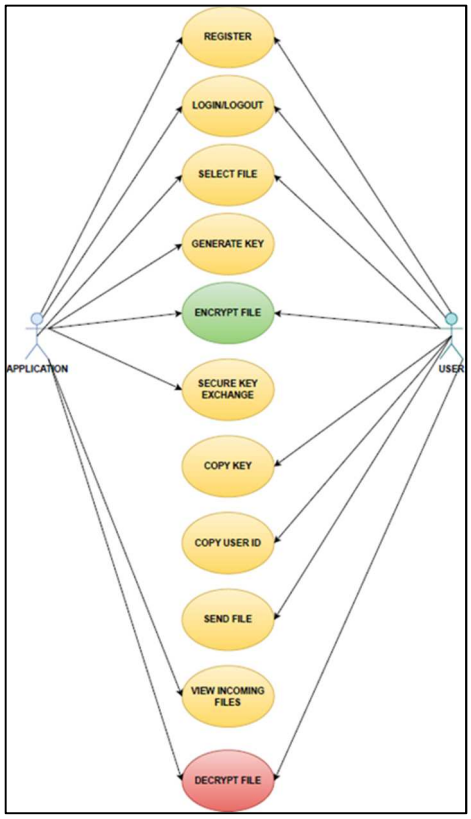

Figure 3: Overall Use Case Diagram of HtCrypt

IV. Results and Discussion

A. Survey

The survey results in Figure 4 show a curious pattern in the use of data encryption applications for securing sensitive data. The majority of people, 75%, have stated that they have previously used such applications, indicating widespread awareness and adoption of security measures among respondents. The 25% who haven't used data encryption applications, on the other hand, raise concerns about potential barriers, concerns, or a lack of awareness about the importance of securing sensitive data. Further investigation into the causes of this divide could provide useful insights into improving cybersecurity awareness and practices.

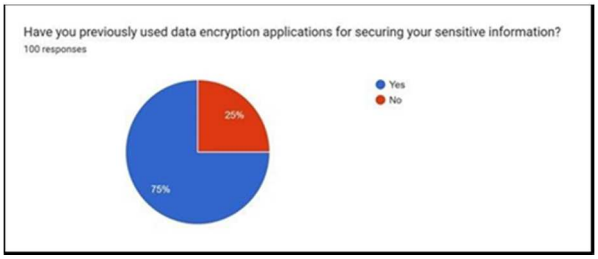

Figure 4: Question on previously used data encryption applications for securing your sensitive information.

The survey findings indicate a clear preference for prioritizing ease of use when considering encryption tools or applications, with 81% of respondents supporting this viewpoint. This suggests that users value user-friendly interfaces and straightforward implementation over complex or intricate encryption solutions. The 19% who do not prioritize ease of use might have specific reasons such as a higher emphasis on advanced features or a willingness to invest more time in mastering intricate tools. Striking a balance between simplicity and robust security features could be crucial for developers and providers of encryption tools to cater to diverse user preferences.

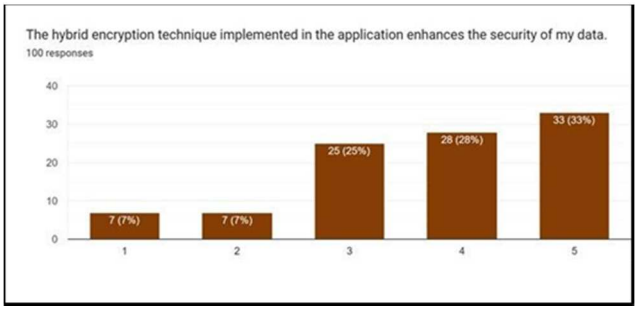

Figure 5: The hybrid encryption technique implemented in the application enhances the security of data.

The survey findings in Figure 5 indicate a diverse range of opinions on the hybrid encryption technique application. While 33% strongly believe it significantly enhances data security, there's a noteworthy 28% expressing a similar sentiment. On the other hand, 25% seem neutral or undecided, and 7% hold a contrasting view. Analyzing these responses can guide us in understanding user perceptions and potentially refining communication or features to address concerns or highlight strengths.

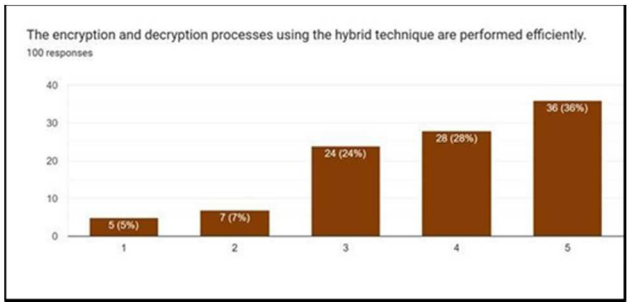

Figure 6: The encryption and decryption processes using the hybrid technique are performed efficiently.

The survey findings in Figure 6 indicate a noteworthy distribution of efficiency ratings for the hybrid encryption and decryption processes. Notably, 36% of respondents find the technique highly efficient (rated 36), while 24% rate it at 24, indicating a substantial positive perception. The 7% and 5% ratings suggest a smaller but still significant portion expressing lower levels of satisfaction. This diverse feedback may warrant further investigation into specific aspects influencing these varied perceptions.

B. Analysis & Application Interface

Headings, The Hybrid Data Encryption Techniques Application is a strategic and advanced solution that improves data security in the digital world. The application ensures a strong safeguard for sensitive information by combining various encryption methods, a user-friendly interface, effectively adapting to evolving threats and mitigating risks [11].

Using strong cryptographic algorithms and dynamic key generation ensures the privacy and security of data. app-to-app data transfer integrity and authentication enhance the transmission security [15]. Moreover, a strong encryption system that can transform plaintext into ciphertext by using asymmetric encryption technique. Overall, the methodology emphasis on hybrid encryption not only strengthens data protection adaptability, but also positions the application as a proactive response to the escalating cybersecurity concerns, establishing it as a valuable asset in the digital realm. Figure 7 shows the method of users to choose a file and specify the desired bit size for encryption. In Figure 8, users can copy and send the private key to the receiver.

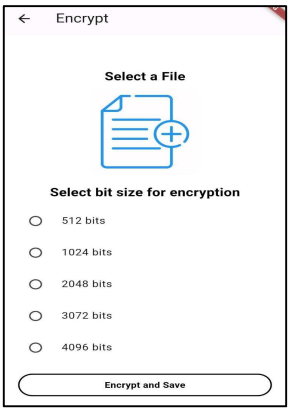

Figure 7: Encrypt Page

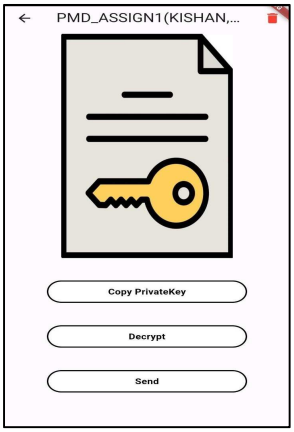

Figure 8: Encryption Page (Copy Key, Send & Decrypt)

V. CONCLUSION

In conclusion, the establishment of a hybrid technique in the domain of data encryption not only signifies a pivotal stride in fortifying security measures but also embodies a strategic approach to strengthening adaptability and resilience in data protection. The integration of diverse encryption methods within this paradigm stands as a proactive measure against potential risks, offering a robust defense mechanism that dynamically adjusts to the evolving landscape of cyber threats. The harmonious amalgamation of various encryption techniques is instrumental in crafting a meticulously designed safeguard for sensitive data, achieving a delicate equilibrium between optimal performance and uncompromising security standards. As we navigate the ever-evolving technological terrain, it becomes evident that the hybrid encryption approach is poised to play a central role in addressing the dynamic challenges inherent in the information age. Its inherent flexibility and efficacy position it as a versatile solution, catering to the nuanced security needs of diverse applications and industries. In essence, the development and ongoing refinement of hybrid encryption herald a promising trajectory in securing data across multiple fronts, underscoring its significance as a formidable and adaptable safeguard in the contemporary digital landscape.

ACKNOWLEDGMENT

It is my utmost pleasure to dedicate this project to my dear parents, who granted me the gift of their unwavering belief in my ability to accomplish this goal. Thank you for your support and patience. I would like to express my greatest gratitude to my supervisor, Ahmad Luqman Bin Ahmad Kamal Ariffin, for her continuous support, encouragement and leadership, who have guide and helped us a lot throughout the whole process of completing this project. Finally, I would like to take this opportunity to thank all my friends and colleagues who have given their support, help and motivation to us, I will be forever grateful.

REFERENCES

[1] BBC News. (2017, October 31). Malaysian data breach sees 46 million phone numbers leaked. BBC News. https://www.bbc.com/news/technology-41816953

[2] Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. Alexandria Engineering Journal, 84, 275–284. https://doi.org/10.1016/j.aej.2023.10.054

[3] Mondal, H. S., Hasan, M. M., Hossain, M. B., Arifin, M. M., & Saha, R. K. (2019). A RSA-Based efficient dynamic secure algorithm for ensuring data security. In Springer eBooks (pp. 643–653). https://doi.org/10.1007/978-981-13-7564-4_54

[4] Dworkin, M. J. (2023, May 9). Advanced Encryption Standard(AES NIST. NIST. https://www.nist.gov/publications/advanced-encryption-standard-aes-0

[5] A new hybrid technique for data encryption. (2015, April 1). IEEE ConferencePublication|IEEEXplore. https://ieeexplore.ieee.org/document/7342801

[6] Adedeji, K. B., & Ponnle, A. A. (2014). A new hybrid data encryption and decryption technique to enhance data security in communication networks:.ResearchGate. https://www.researchgate.net/publication/303497916_A_New_Hybrid_Data_Encryption_and_Decryption_Tech nique_to_Enhance_Data_Security_in_Communication_ Networks_Algorithm_Development

[7] [7] Al-Attab, S. (2017). Hybrid Data Encryption Technique for Data SecurityinCloudComputingBaseL. https://www.semanticscholar.org/paper/Hybrid-Data-Encryption-Technique-for-Data-Security-Al-Attab/5ed46ea2ee881f33f44c90e57ae52c5cc36c2c1f

[8] [8] Zhang, Q. (2021, January). An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption. In 2021 2nd international conference on computing and data science (CDS) (pp. 616-622). IEEE.

[9] [9] Orobosade, A., Favour-Bethy, T. A., Kayode, A. B., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. Communications on Applied Electronics, 7(33), 25-31.

[10] Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6), 31-37.

[11] Vashi, D., Bhadka, H. B., Patel, K., & Garg, S. (2020). An Efficient hybrid approach of attribute based encryption for privacy preserving through horizontally partitioned data. Procedia Computer Science, 167, 2437-2444.

[12] Kumar, A., Jain, V., & Yadav, A. (2020, February). A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In 2020 international conference on power electronics & IoT applications in renewable energy and its control (PARC) (pp. 514-517). IEEE.

[13] Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid cryptographic approach for internet ofhybrid cryptographic approach for internet ofthings applications: A review. Journal of Information and Communication Technology, 19(3), 279-319.

[14] Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 80, 21165-21202.

[15] Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020 (pp. 537-547). Springer Singapore.

[16] Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. International Journal of Advanced Computer Science and Applications, 12(6), 31-37.

[17] Ishak, Z., Rajendran, N., Al-Sanjary, O. I., & Razali, N. A. M. (2020, February). Secure biometric lock system for files and applications: a review. In 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 23-28). IEEE