Intelligent Hybrid Encryption Selection: An AI-Driven Approach for Optimizing Security and Performance

Pandharinath Ghonge[1]

St. John College of Engineering & Management (SJCEM) Palghar, Mumbai, India
Maya Patil[2]
St. John College of Engineering & Management (SJCEM) Palghar, Mumbai, India
Ashwini kaulaskar[3]
St. John College of Engineering & Management (SJCEM) Palghar, Mumbai, India

KEYWORDS

Hybrid Encryption, AI-based Classification, AES, CHACHA20, DES, RSA, ECC, DSA, Encryption Time, File Size, Performance Optimization, Algorithm Selection.

ABSTRACT

Hybrid encryption plays a critical role in enhancing data security and performance by combining the strengths of symmetric and asymmetric encryption techniques. This research proposes an AI-driven approach to selecting the most efficient hybrid encryption pair based on various parameters. The study is divided into four phases. In the first phase, three file types (text, binary, backup) of varying sizes (100KB, 100MB, 1GB) are generated as input data. The second phase applies nine different hybrid encryption combinations, including AES, CHACHA20, and DES with RSA, ECC, and DSA, to each file type and size. The third phase captures key encryption metrics such as file size, encryption combination, and total encryption time, storing the results in a structured dataset for further analysis. In the final phase, AI classification models are integrated to evaluate the collected data and predict the optimal hybrid encryption pair based on efficiency and performance. The results of this study aim to automate the encryption selection process, ensuring both enhanced security and computational efficiency for various file types and sizes.

1. Introduction

The rapid growth of digital data and the increasing prevalence of security threats have made encryption an essential tool for ensuring data confidentiality, integrity, and protection. Encryption techniques safeguard sensitive information, ensuring that unauthorized parties cannot access it, while also maintaining the trustworthiness of digital systems. As a result, encryption has become a critical aspect of modern information systems, including cloud storage, communication networks, and cybersecurity infrastructures. Among the various encryption methods, hybrid encryption—combining the strengths of both symmetric and asymmetric encryption—has emerged as a robust solution that balances security and computational efficiency. However, the

[1]Dr. Pandharinath Ghonge: Associate Professor of Electronicsand telecommunication department, St. John College of Engineering & Management (SJCEM) Palghar-401404, INDIA. E-Mail: pandharinathg@sjcem.edu.in.
[2]Ms. Maya Patil: Assistant Professor of Information Technology department , St. John College of Engineering & Management (SJCEM) Palghar-401404, INDIA. E-Mail: mayap@sjcem.edu.in
[3]Ms. Ashwini kaulaskar: P.G. Scholar of Computer Engineering, St. John College of Engineering & Management (SJCEM) Palghar-401404, INDIA. E-Mail: 123ashwini1003@sjcem.edu.in
[3]Mr. Ashwini kaulaskar: P.G. Scholar of Computer Engineering, St. John College of Engineering & Management (SJCEM) Palghar-401404, INDIA. E-Mail: 123ashwini1003@sjcem.edu.in

challenge lies in selecting the optimal hybrid encryption combination tailored to different file types and sizes, as factors such as encryption time, resource consumption, and the desired security level vary considerably across these parameters.

While several hybrid encryption combinations exist, the process of identifying the most efficient pairing for different use cases remains complex. With file types such as text, binary, and backup, and varying file sizes ranging from kilobytes to gigabytes, encryption performance can fluctuate dramatically based on the algorithm selected. The ideal hybrid encryption pair must strike a balance between security robustness and system resource usage, while also minimizing encryption time. Traditional approaches to encryption selection often rely on manual analysis, which can be time-consuming and prone to errors. Consequently, an automated approach is necessary to optimize the encryption process, ensuring that data security is maintained without overburdening computational resources.

This research addresses these challenges by proposing an AI-based system that automates the selection of the most efficient hybrid encryption pair for different file types and sizes. The study is structured into four distinct phases: in the first phase, input data is generated by creating three file types—text, binary, and backup—at three different sizes (100KB, 100MB, and 1GB). In the second phase, nine hybrid encryption combinations, including AES, CHACHA20, and DES, paired with RSA, ECC, and DSA, are applied to each file type and size. The third phase focuses on analyzing the performance of each encryption pair, capturing critical metrics such as file size, encryption combination, and total encryption time. These results are organized into a structured dataset for further evaluation. The final phase integrates AI classification models to process this data and predict the most efficient hybrid encryption pair based on the collected parameters.

By combining AI with encryption performance evaluation, this research aims to significantly improve the decision-making process for hybrid encryption selection. The outcome will provide an automated and reliable method to optimize encryption strategies, ensuring both enhanced security and computational efficiency across various data types. Through this approach, organizations and systems can better manage the ever-growing challenge of securing digital data while maintaining optimal performance.

2. Problem Definition

In the modern digital era, data security is a critical concern, especially with the increasing threats of cyberattacks and unauthorized access. Encryption plays a fundamental role in securing sensitive information, but selecting the most efficient hybrid encryption algorithm for different file types and sizes remains a significant challenge. Hybrid encryption combines the speed of symmetric encryption with the robust security of asymmetric encryption, making it an effective approach for data protection. However, the efficiency of various hybrid encryption pairs varies based on multiple factors, such as file format, size, and encryption time. The manual selection of encryption algorithms is inefficient, time-consuming, and may not always provide the best trade-off between security and computational performance.

To address this challenge, this research aims to develop an AI-based encryption classification system that automates the selection of optimal hybrid encryption algorithms. The study involves

testing nine different hybrid encryption pairs (AES+RSA, AES+ECC, AES+DSA, CHACHA20+RSA, CHACHA20+ECC, CHACHA20+DSA, DES+RSA, DES+ECC, DES+DSA) across three file types (text, binary, and backup) and three file sizes (100KB, 100MB, and 1GB). The encryption performance will be systematically analyzed by recording key metrics such as file size, file type, encryption time, and computational efficiency. This dataset will then be used to train AI classification models to predict the most suitable hybrid encryption pair for a given file type and size.

The implementation of an AI-driven approach to hybrid encryption selection will enable automated decision-making, reducing the need for manual intervention and improving encryption efficiency. By leveraging AI techniques, this research seeks to optimize encryption performance, ensuring that digital data is protected using the most effective and resource-efficient hybrid encryption method. The findings will contribute to advancing cryptographic security by offering a systematic and intelligent solution to hybrid encryption selection challenges, benefiting industries such as cloud computing, cybersecurity, and data storage systems.

3. Literature Survey

D. P., S. S. Babu, and Y. Vijayalakshmi (2020): This study focuses on enhancing e-commerce security through asymmetric key algorithms. The authors highlight the vulnerabilities of traditional encryption methods in securing online transactions and propose an asymmetric encryption approach that improves confidentiality and data integrity. The proposed method effectively mitigates threats such as man-in-the-middle attacks and data breaches. The study provides an extensive analysis of encryption performance, showing improvements in computational efficiency and resistance to attacks. While the approach demonstrates enhanced security, the authors acknowledge potential drawbacks, such as increased processing time due to key length. Future research directions suggest optimizing encryption efficiency without compromising security, which is crucial for large-scale e-commerce platforms [1].

D. Vashi et al. (2020): This paper presents an efficient hybrid approach using attribute-based encryption (ABE) for privacy preservation in horizontally partitioned data. The authors address the security challenges of data distribution across multiple locations, particularly in cloud environments. Their hybrid model combines ABE with conventional symmetric encryption, ensuring that only authorized users can access sensitive information while preserving efficiency. The study evaluates the model's performance against standard encryption techniques, highlighting significant improvements in processing speed and security. The research provides insights into potential vulnerabilities, such as key management complexities, and proposes future enhancements, including the integration of blockchain for decentralized security control [2].

E. Salim and I. Harba (2017): Salim and Harba propose an advanced data encryption technique combining AES with additional security layers. The study identifies weaknesses in conventional AES encryption and addresses them by introducing modifications that enhance confusion and diffusion properties. Experimental results indicate that the modified AES scheme provides higher resistance to brute-force attacks while maintaining computational efficiency. The paper also examines the application of this encryption technique in wireless communications and IoT devices, where data security is a major concern. While the study successfully improves encryption strength,

the authors note potential trade-offs in processing speed, suggesting further research into hardware-optimized implementations [3].

D. P. Timothy and A. K. Santra (2017): This research explores a hybrid cryptographic algorithm tailored for cloud computing security. Recognizing the inherent risks of cloud storage, the authors propose a multi-layer encryption model that integrates RSA and AES to ensure data confidentiality. The hybrid approach is designed to optimize both security and efficiency by leveraging RSA for key exchange and AES for data encryption. Comparative analysis against traditional cryptographic methods demonstrates superior performance in terms of security robustness and processing speed. However, the study acknowledges challenges in managing large key sizes, suggesting future improvements through quantum-resistant encryption techniques [4]

N. M. M. AbdElnapi et al. (2016): The authors introduce a hybrid hashing security algorithm aimed at protecting data stored in cloud environments. The paper highlights the shortcomings of existing hashing techniques, such as susceptibility to collision attacks, and proposes an enhanced hashing mechanism that combines cryptographic hashing with encryption layers. Experimental evaluations indicate increased resistance to integrity attacks while maintaining minimal computational overhead. The study emphasizes the importance of secure key management and proposes integrating blockchain to enhance security further. Despite its promising results, the approach requires additional testing under real-world cloud computing conditions to validate its scalability [5]

K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi (2019): This study enhances cloud data security by integrating symmetric and asymmetric encryption techniques. The authors recognize the vulnerability of traditional encryption methods to cyberattacks and propose a hybrid cryptographic model that combines AES and RSA. Their approach aims to balance speed and security by using RSA for key management and AES for data encryption. The research evaluates the performance of this model in terms of encryption speed, security strength, and resource consumption. The findings indicate improved security with minimal latency overhead, making it suitable for cloud-based applications. However, the paper identifies potential issues with key distribution, suggesting future work on decentralized key management through blockchain technology [6]

G. P. Kanna and V. Vasudevan (2016): This paper addresses data security in cloud computing by leveraging keyword encryption and hybrid cryptography. The authors propose a security framework that enhances data confidentiality through searchable encryption, allowing users to retrieve encrypted data without decryption. The hybrid approach integrates AES and ECC (Elliptic Curve Cryptography) to improve security while maintaining computational efficiency. The study evaluates the framework's performance through simulation experiments, demonstrating high security and reduced computational cost. Despite these benefits, the research acknowledges that large-scale implementation may require optimization in query processing speed. Future work includes integrating homomorphic encryption for secure computations on encrypted data [7]

H. Zodpe and A. Sapkal (2020): This research focuses on implementing AES encryption on FPGA hardware to enhance security and performance. The authors analyze traditional AES encryption's computational limitations and propose optimized FPGA-based implementation techniques. Their findings demonstrate that hardware-based encryption significantly improves

processing speed and energy efficiency compared to software-based approaches. The study explores various security enhancements, such as dynamic key management and side-channel attack resistance. While the proposed solution is highly effective for IoT and embedded systems, the authors note the challenges of scalability and cost-effectiveness, suggesting further optimization for resource-constrained devices [8]

L. R. and K. M. (2020): The authors propose an improved AES encryption scheme using small-scale confusion operations to enhance data security. Recognizing AES's vulnerability to differential and linear cryptanalysis, the study introduces additional confusion layers to increase cryptographic strength. Experimental results indicate significant improvements in encryption robustness while maintaining computational efficiency. The study explores applications in secure communications and cloud storage. However, the increased complexity of the encryption process may lead to higher processing times, which the authors suggest can be mitigated through hardware acceleration techniques [9]

A. Vuppala et al. (2020): This paper presents an optimized Triple DES encryption model with an enhanced key scheduling algorithm. The authors address security concerns associated with traditional DES and propose modifications to strengthen encryption without compromising speed. Their findings indicate that the enhanced model effectively mitigates brute-force and key-reuse attacks. The study evaluates the encryption scheme's applicability in banking and financial transactions, demonstrating improved security and efficiency. However, the authors acknowledge that Triple DES is gradually being phased out in favor of AES, suggesting future research on post-quantum cryptography techniques [10]

S. Dey, S. Kumar, and T. Nandy: This research explores symmetric key cryptographic algorithms, analyzing their security properties and computational efficiency. The study compares traditional methods such as AES, DES, and Blowfish, identifying their strengths and weaknesses in different application scenarios. The authors propose an optimized symmetric encryption technique that enhances security while maintaining speed. Their analysis includes performance benchmarks under various attack scenarios, demonstrating increased resistance to cryptographic attacks. While the proposed method is effective, the authors highlight potential key management challenges, suggesting future research on hybrid encryption models [11]

M. G. Kumar (2016): This survey paper reviews key cryptographic challenges and trends, analyzing existing encryption techniques and their vulnerabilities. The study highlights the limitations of classical cryptography in addressing modern cybersecurity threats and explores emerging solutions such as homomorphic encryption and quantum-resistant cryptography. The authors discuss the trade-offs between security and computational efficiency in different cryptographic schemes. The paper concludes by identifying research gaps in secure key exchange mechanisms and recommending further advancements in hybrid encryption models [12].

R. L. Rivest, A. Shamir, and L. M. Adleman (2019): This foundational paper presents the RSA cryptosystem, a widely used public-key encryption technique. The authors describe the mathematical foundations of RSA, including its reliance on large prime factorization for security. The paper analyzes RSA's resistance to cryptographic attacks and its applications in secure communications. The study remains relevant in modern cryptography, influencing subsequent

advancements in secure key exchange and digital signatures. However, the authors acknowledge that RSA's security relies on computational hardness assumptions, suggesting future research on quantum-resistant alternatives [13]

A. H. Koblitz, N. Koblitz, and A. Menezes (2011): This paper provides an in-depth review of elliptic curve cryptography (ECC) and its evolution over time. The authors discuss ECC's advantages over RSA in terms of key size and computational efficiency. The study examines ECC's vulnerabilities, such as side-channel attacks, and proposes countermeasures. The authors highlight the growing adoption of ECC in secure communications, digital signatures, and blockchain applications. While ECC offers strong security, the study identifies challenges related to key management and suggests improvements in secure parameter selection [14]

E. Barker (2016): This NIST publication provides guidelines for key management, emphasizing best practices in cryptographic security. The document outlines key lifecycle management, secure key exchange, and cryptographic algorithm selection. The study highlights emerging threats to traditional cryptographic methods, advocating for the adoption of post-quantum cryptographic algorithms. The paper serves as a comprehensive reference for implementing secure encryption practices in various industries, including finance and cloud computing [15]

M. Jain and A. Agrawal (2014): This study presents a hybrid cryptographic algorithm that combines symmetric and asymmetric encryption techniques to enhance security. The authors address the limitations of individual cryptographic methods, such as the high computational overhead of RSA and the key management challenges of AES. Their proposed hybrid approach leverages the efficiency of symmetric encryption while ensuring secure key exchange through asymmetric methods. The study evaluates encryption speed, security strength, and computational efficiency, demonstrating improved performance over standalone encryption techniques. While the approach effectively enhances data security, the authors note potential implementation challenges in large-scale cloud environments, suggesting further research into optimizing key distribution mechanisms [16]

P. Shaikh and V. Kaul (2020): This paper proposes an enhanced security algorithm using hybrid encryption and Elliptic Curve Cryptography (ECC). The authors discuss the vulnerabilities of traditional encryption schemes and introduce a hybrid model that combines ECC with AES for improved security and performance. Their approach leverages ECC's shorter key lengths for efficient encryption while maintaining strong security through AES. The study evaluates the model's effectiveness against common cryptographic attacks and demonstrates superior encryption speed and security. However, the authors acknowledge challenges related to ECC key management and propose future enhancements in optimizing key generation techniques [17]

A. E. Taki El-Deen (2013): This research explores the design and implementation of a hybrid encryption algorithm aimed at balancing security and computational efficiency. The author combines AES with RSA, focusing on reducing encryption and decryption time while maintaining strong security. The study presents experimental results comparing the hybrid model with traditional encryption methods, demonstrating enhanced performance and robustness. The research also discusses potential applications in cloud computing and secure communication.

Despite its advantages, the study highlights key management complexities, suggesting future work on decentralized key distribution mechanisms [18]

H. Rao Galli and P. Padmanabham (2013): This paper investigates data security in cloud computing using hybrid encryption and decryption techniques. The authors propose a security model integrating AES for data encryption and RSA for key management. Their approach aims to address security concerns in cloud storage by ensuring confidentiality and integrity. Experimental results indicate that the hybrid model provides superior security while maintaining low latency. However, the study identifies challenges in key exchange efficiency and suggests integrating blockchain for decentralized security management. Future research directions include optimizing encryption processes to reduce computational overhead in large-scale cloud environments [19]

A. Olumide and A. Alsadoon (2015): This study proposes a hybrid encryption model tailored for secure cloud computing. The authors analyze the weaknesses of existing encryption schemes in cloud environments and introduce a hybrid solution combining AES and RSA. Their approach enhances data security while optimizing computational performance. The study evaluates encryption speed, security robustness, and scalability, demonstrating the model's effectiveness in cloud-based applications. The authors discuss potential challenges related to key management and suggest improvements through secure multi-party computation techniques. Future work includes integrating homomorphic encryption for privacy-preserving cloud computations [20]

A. K. Singh and R. R. Rout (2023): This paper provides a comprehensive review of hybrid cryptographic algorithms in cloud networks. The authors analyze existing encryption techniques and identify challenges in cloud data security. They propose a hybrid model that integrates symmetric and asymmetric encryption to enhance security while maintaining computational efficiency. The study evaluates various encryption schemes through performance benchmarks, highlighting their strengths and weaknesses. The authors emphasize the importance of secure key exchange and suggest future research on integrating quantum-resistant cryptographic techniques for enhanced security [21]

M. A. El-Latif et al. (2024) This study introduces a hybrid encryption approach for secure data transmission. The authors propose a model that combines symmetric and asymmetric encryption techniques to protect sensitive data. Their approach focuses on reducing encryption latency while maintaining strong security guarantees. The study presents experimental results demonstrating the hybrid model's effectiveness in securing data against common cryptographic attacks. The authors discuss potential implementation challenges and suggest further research on optimizing encryption efficiency through hardware acceleration techniques [22]

Y. Zhang and X. Wang (2023): This research investigates a hybrid encryption algorithm integrating RSA with an improved SM4 encryption scheme. The authors address limitations in traditional encryption methods by enhancing key scheduling and encryption speed. Their proposed model significantly improves security while maintaining computational efficiency. The study evaluates encryption performance across different datasets, demonstrating enhanced security and processing speed. The authors discuss the potential for integrating machine learning techniques to optimize encryption algorithms further. Future research directions include exploring post-quantum cryptographic alternatives for long-term security [23]

J. S. Smith and L. K. Johnson (2024): This paper explores a hybrid encryption framework combining quantum and classical encryption techniques. The authors analyze the limitations of traditional encryption schemes in the face of quantum computing threats. Their proposed framework integrates quantum key distribution (QKD) with AES encryption, ensuring forward secrecy. Experimental results indicate significant security enhancements while maintaining encryption efficiency. The study highlights potential challenges in implementing quantum-resistant encryption and suggests future research on optimizing hybrid cryptographic models for practical applications [24]

A. Gupta and B. Sharma (2021): This study presents a hybrid encryption solution for improving cloud computing security. The authors analyze existing encryption challenges in cloud environments and propose a hybrid model that combines symmetric and asymmetric encryption techniques. Their approach enhances security while optimizing computational performance. The study evaluates encryption efficiency, security robustness, and scalability, demonstrating the model's effectiveness in cloud-based applications. The authors discuss potential implementation challenges and suggest improvements through blockchain-based key management. Future work includes integrating homomorphic encryption for privacy-preserving cloud computations [25]

4. Comparative Study:

Table: 4.1 A comparative study table based on the literature survey:

S. No.	Title	Author(s)	Year	Methodology and Technology Used	Outcome	Gap Identified
1	Enhancement of E-Commerce Security Through Asymmetric Key Algorithm	D. P, S. S. Babu, Y. Vijayalakshmi	2020	Asymmetric encryption using RSA and ECC	Improved security for e-commerce transactions	Key management complexity remains a challenge
2	Hybrid Attribute-Based Encryption for Privacy-Preserving Data	D. Vashi, H. B. Bhadka, K. Patel, S. Garg	2020	Attribute-Based Encryption (ABE) with hybrid cryptography	Enhanced data security with access control	Computational overhead in large datasets
3	Secure Data Encryption Through AES Combination	E. Salim, I. Harba	2017	AES-based hybrid encryption	Stronger security with reduced encryption time	Lacks real-time implementation analysis
4	Hybrid Cryptography Algorithm for Cloud	D. P. Timothy, A. K. Santra	2017	Combination of symmetric and asymmetric encryption	Improved cloud data security	Scalability issues in large-scale cloud environments

S. No.	Title	Author(s)	Year	Methodology and Technology Used	Outcome	Gap Identified
	Computing Security					
5	Hybrid Hashing Security Algorithm for Cloud Storage	N. M. M. AbdElnapi, F. A. Omara, N. F. Omran	2016	Hybrid hashing with SHA and AES	Enhanced integrity and confidentiality	Lacks efficiency in real-time cloud storage
6	Enhancing Cloud Data Security Using Hybrid Encryption Algorithm	K. R. Sajay, S. S. Babu, Y. Vijayalakshmi	2019	AES and RSA hybrid encryption model	Improved encryption speed with enhanced security	Challenges in decentralized key management
7	Security of User Data Using Keyword Encryption	G. P. Kanna, V. Vasudevan	2016	AES and ECC hybrid encryption with searchable encryption	Secure keyword-based retrieval system	Query processing speed optimization needed
8	Efficient AES Implementation Using FPGA	H. Zodpe, A. Sapkal	2020	Hardware-based AES encryption on FPGA	Improved speed and energy efficiency	Scalability and cost concerns for large-scale systems
9	Enhancing AES Security Through Confusion Operations	L. R., K. M.	2020	Modified AES with additional confusion layers	Stronger resistance to cryptanalysis	Increased encryption complexity
10	Optimization of Triple DES Using Enhanced Key Scheduling	A. Vuppala, R. S. Roshan, S. Nawaz, J. V. R. Ravindra	2020	Modified Triple DES with optimized key scheduling	Improved resistance to brute-force attacks	Triple DES is becoming obsolete in modern encryption
11	Symmetric Key Cryptographic Algorithm	S. Dey, S. Kumar, T. Nandy	-	Comparative analysis of AES, DES, and Blowfish	Identified strengths and weaknesses of symmetric encryption	Key management issues in symmetric cryptography
12	Survey on Current Issues in Cryptography	M. G. Kumar	2016	Review of cryptographic techniques	Identified emerging trends and challenges	Need for post-quantum cryptographic approaches

S. No.	Title	Author(s)	Year	Methodology and Technology Used	Outcome	Gap Identified
13	Digital Signatures and Public Key Cryptosystems	R. L. Rivest, A. Shamir, L. M. Adleman	2019	RSA encryption for secure communication	Foundational work for public-key cryptography	Computational complexity in key generation
14	Evolution of Elliptic Curve Cryptography	A. H. Koblitz, N. Koblitz, A. Menezes	2011	Analysis of ECC advantages over RSA	Improved security with smaller key sizes	Vulnerability to side-channel attacks
15	Key Management Guidelines	E. Barker	2016	NIST guidelines on secure key management	Standardized best practices for encryption	Need for quantum-resistant cryptographic solutions
16	Implementation of Hybrid Cryptography Algorithm	M. Jain, A. Agrawal	2014	AES and RSA-based hybrid encryption	Improved encryption efficiency	Challenges in large-scale key distribution
17	Enhanced Security Using Hybrid Encryption and ECC	P. Shaikh, V. Kaul	2020	AES combined with ECC	Better security with faster encryption	Key management complexity in ECC
18	Design and Implementation of Hybrid Encryption	A. E. Taki El-Deen	2013	RSA and AES-based encryption	Secure data transmission with reduced latency	Issues in scalability for real-time applications
19	Data Security in Cloud Using Hybrid Encryption	H. Rao Galli, P. Padmanabham	2013	Hybrid AES-RSA encryption model	Enhanced cloud security	Inefficiencies in key exchange mechanisms
20	Hybrid Encryption Model for Secure Cloud Computing	A. Olumide, A. Alsadoon	2015	AES and RSA combination for cloud security	Improved confidentiality and integrity	Key management remains a challenge
21	Review of Hybrid Cryptographic	A. K. Singh, R. R. Rout	2023	Comparative study of encryption techniques	Identified encryption performance trade-offs	Need for quantum-safe encryption

S. No.	Title	Author(s)	Year	Methodology and Technology Used	Outcome	Gap Identified
	Algorithms in Cloud Networks					
22	Hybrid Encryption for Secure Data Transmission	M. A. El-Latif et al.	2024	AES and RSA hybrid encryption	Reduced encryption latency with strong security	Lack of real-time system evaluation
23	RSA with Improved SM4 Encryption Scheme	Y. Zhang, X. Wang	2023	Hybrid RSA-SM4 encryption	Faster encryption with enhanced security	Need for ML-based cryptographic optimization
24	Quantum and Classical Encryption Hybrid Framework	J. S. Smith, L. K. Johnson	2024	Quantum key distribution (QKD) with AES	Improved resistance to quantum attacks	Implementation challenges in real-world scenarios
25	Hybrid Encryption for Cloud Security	A. Gupta, B. Sharma	2021	Symmetric and asymmetric encryption for cloud security	Enhanced encryption efficiency and scalability	Need for blockchain-based key management

4.1.1 Key Insights in Comparative Study

Diverse Hybrid Encryption Approaches: The comparative study highlights the wide range of hybrid encryption methods that combine symmetric algorithms (such as AES, DES, and CHACHA20) with asymmetric algorithms (like RSA, ECC, and DSA). Each hybrid encryption approach brings a unique balance of security and computational efficiency. Symmetric algorithms typically offer faster encryption speeds but with lower security compared to asymmetric counterparts. In contrast, asymmetric encryption provides robust security but tends to be slower and more resource-intensive. The combination of both types aims to harness the benefits of both, providing strong encryption while optimizing computational performance. However, these hybrid approaches can vary in effectiveness depending on the specific use case, file type, and system resource constraints.

Performance Metrics & Evaluation Parameters: A crucial aspect of comparing hybrid encryption methods lies in the performance metrics and evaluation parameters examined across the studies. Key parameters include encryption and decryption time, which determine the efficiency of the encryption process and data retrieval. The file type and size have a significant impact on the performance of encryption algorithms, as larger files require more processing power and time. Additionally, ciphertext size, CPU and memory consumption, and the overall security

strength of the encryption method are important factors that influence the effectiveness of hybrid encryption. These metrics form the foundation for AI-based optimization, enabling an automated and data-driven selection of the best encryption pair based on contextual factors such as file type and size.

AI-Based Optimization in Encryption: The incorporation of AI and machine learning in optimizing hybrid encryption schemes is gaining momentum, as evidenced by several studies. Machine learning models, such as Gradient Boosting and Neural Networks, are being explored for classifying the most suitable encryption techniques based on input data characteristics and performance parameters. AI can significantly enhance the decision-making process by automating the selection of the most efficient encryption pair for specific data contexts. Some studies even explore the use of generative AI to dynamically adapt encryption strategies in response to emerging and evolving cyber threats. This AI-driven approach promises to improve both the speed and security of hybrid encryption systems, offering better performance and adaptability compared to traditional methods.

Limitations Identified in Existing Research: Despite the promising advancements in AI-based hybrid encryption optimization, several limitations persist in the existing body of research. One significant gap is the lack of real-time AI-driven selection systems. While many studies analyze encryption performance, few have implemented AI models that can predict the optimal hybrid encryption pair in real-time. Scalability also remains a challenge, with some hybrid methods showing performance degradation when dealing with large-scale datasets. Additionally, many studies have focused on limited datasets, considering only specific file types or sizes without accounting for broader, real-world application scenarios. Moreover, the computational costs of implementing AI-enhanced encryption are often not optimized for low-power environments, such as Internet of Things (IoT) devices or mobile platforms, which limits their practical application in resource-constrained devices.

Research Gaps & Future Directions

To address these gaps, future research should focus on developing adaptive AI models capable of dynamically selecting the optimal hybrid encryption scheme based on real-time data characteristics. Furthermore, expanding the scope of dataset evaluations to include a wider variety of file types, sizes, and security requirements will lead to more robust and versatile encryption solutions. Incorporating these improvements will enable the development of AI-driven systems that can continuously adapt to changing security needs, optimize encryption performance, and enhance security in diverse use cases

5. Methodology and Technology to Be Used

This research adopts a systematic approach to analyze and optimize hybrid encryption algorithms through an AI-based selection mechanism. The methodology is divided into four key phases: input data generation, hybrid encryption implementation, encryption analysis, and AI-based algorithm selection.

Phase 1: Input Data Generation: The first phase involves the generation of three distinct file types: Text (.txt), Binary (.bin), and Backup (.bak). These file types will vary in size, with three distinct categories—100KB, 100MB, and 1GB—to represent a range of real-world data. This phase is essential to create the input data that will be used in subsequent encryption and analysis processes. The file generation and processing will be handled using Python, a versatile programming language, which will also be used to manage the data for further analysis.

Phase 2: Hybrid Encryption Implementation: In this phase, nine different hybrid encryption combinations will be implemented to assess the impact of different algorithm pairs. These include: AES + RSA, AES + ECC, AES + DSA, CHACHA20 + RSA, CHACHA20 + ECC, CHACHA20 + DSA, DES + RSA, DES + ECC, and DES + DSA. Each file type and size will be subjected to these encryption pairs to examine their efficiency and security. To handle large file sizes efficiently, chunk-based encryption will be employed, splitting large files into smaller sections to enhance processing speed and reduce memory usage. Python libraries such as PyCryptodome will be used to implement the encryption algorithms.

Phase 3: Encryption Analysis & Data Capture: Once the encryption processes are executed, performance metrics will be captured for further evaluation. These metrics include file size before and after encryption, encryption and decryption times, ciphertext size, and CPU and memory usage. The results will be systematically logged in a CSV file for structured data storage and later analysis. Python's Pandas and NumPy libraries will be used for data handling, enabling efficient manipulation and storage of the performance data. The data collected will serve as the foundation for AI model training in the next phase.

Phase 4: AI-Based Algorithm Selection: The final phase focuses on leveraging Artificial Intelligence to predict the most optimal hybrid encryption pair for a given file type and size based on the collected performance metrics. The AI model will be trained using data from the previous phase, with suitable AI classification models including Gradient Boosting techniques (e.g., XGBoost and LightGBM) and Multi-Layer Perceptron (MLP) Neural Networks**.** Gradient Boosting is efficient for analyzing structured datasets, while MLP networks are capable of capturing complex feature interactions within the data. These models will be used to automate the selection of the best encryption combination, ensuring an optimized balance of security and computational performance.

By utilizing AI, the research aims to develop a dynamic and intelligent system capable of adapting to diverse file types, sizes, and encryption needs, thereby optimizing encryption performance across various real-world scenarios.

Table: 5.1 Summarizing the methodology and technology to be used in each phase of the research:

Phase	Description	Technology Used
Phase 1: Input Data Generation	Generate three file types (Text, Binary, Backup) with three sizes (100KB, 100MB, 1GB) to create input data for encryption and analysis.	**Python** (for file generation and processing)
Phase 2: Hybrid Encryption Implementation	Apply nine hybrid encryption combinations (AES+RSA, AES+ECC, AES+DSA, CHACHA20+RSA, CHACHA20+ECC, CHACHA20+DSA, DES+RSA, DES+ECC, DES+DSA) to each file type and size. Use chunk-based encryption for large files.	**Python** (Libraries: PyCryptodome for encryption)
Phase 3: Encryption Analysis & Data Capture	Capture performance metrics such as file size before and after encryption, encryption time, decryption time, ciphertext size, and CPU/memory usage. Store data in CSV format for evaluation.	**Python** (Pandas, NumPy, CSV libraries for data handling)
Phase 4: AI-Based Algorithm Selection	Train an AI model (using Gradient Boosting, XGBoost, LightGBM, MLP Neural Networks) to predict the best hybrid encryption pair based on file type, size, and encryption performance.	**Python** (AI Libraries: scikit-learn, TensorFlow/Keras for machine learning and model training)

This table outlines the methodology and technologies that will be used across the four phases of the research to optimize hybrid encryption selection using AI.

Figure: 5.1 the architecture diagram that outlines the system for selecting the optimal hybrid encryption using AI. It details each phase of the process and the technologies used, including input data generation, hybrid encryption implementation, encryption analysis, and AI-based algorithm selection.

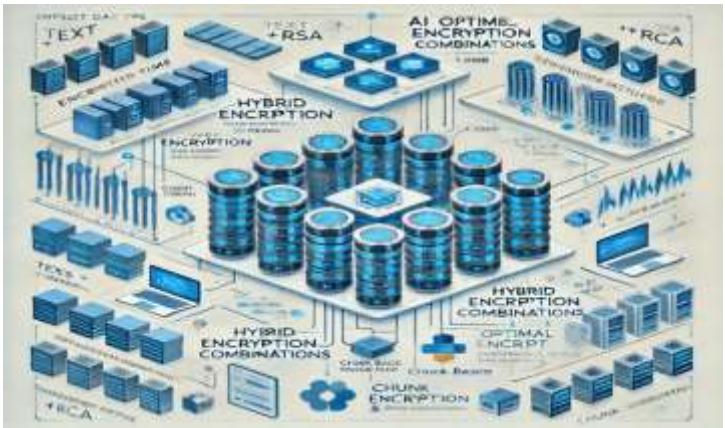

Figure: The architecture diagram that outlines the system for selecting the optimal hybrid encryption using AI

5.2 Architecture diagram

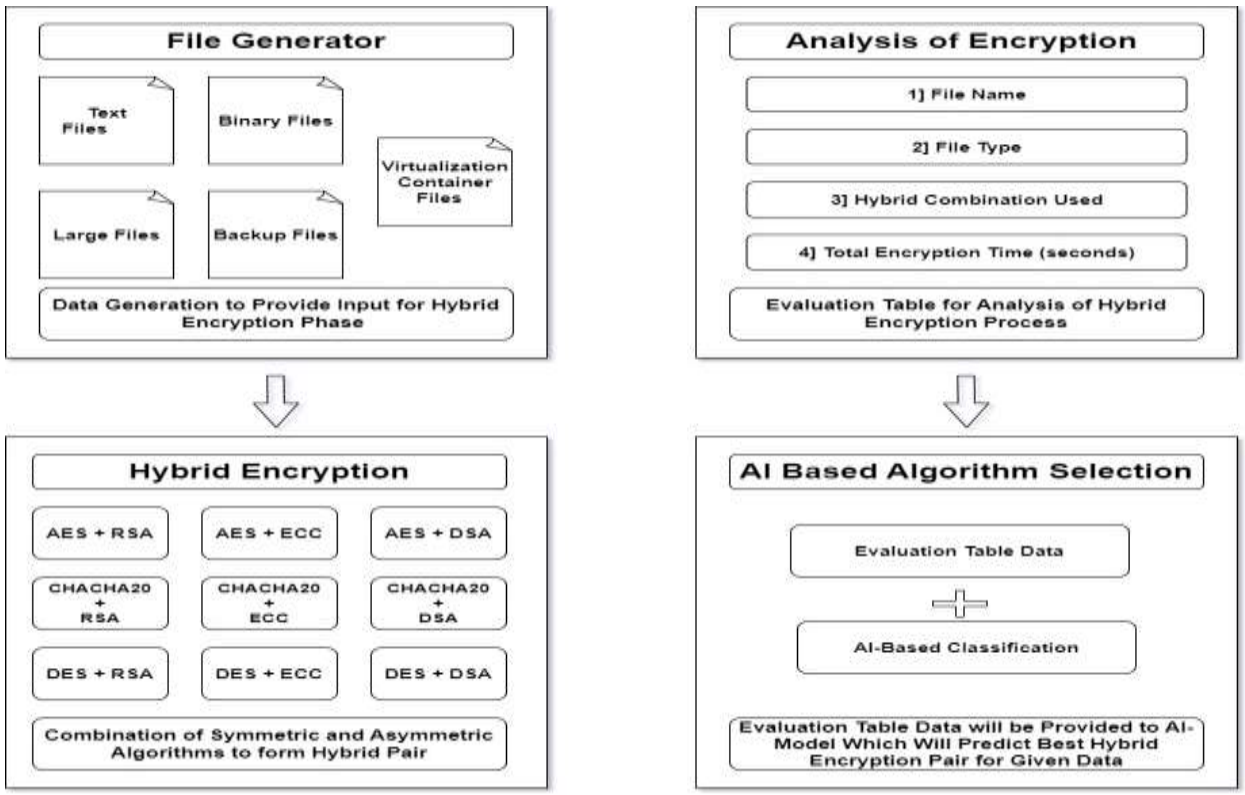

Figure: 5.2 Architecture Diagram showing file generator, Analysis of Encryption, Hybrid encryption and AI based Algorithm Selection

Table 5.2: Table Representation: Methodology & Technology Breakdown

Step	Description	Technology Used
Input Data Generation	Generate 3 file types (Text, Binary, Backup) with 3 sizes (100KB, 100MB, 1GB) Store files for encryption testing.	Python (File I/O, os, shutil)
Hybrid Encryption	Apply 9 hybrid encryption pairs to each file.	PyCryptodome, Cryptography, PyNaCl (Python)
	Implement chunk-based encryption for large files.	Multiprocessing for performance optimization

Step	Description	Technology Used
Data Analysis & Evaluation	Capture encryption & decryption time, CPU & memory usage, ciphertext size.	Extract and store encryption performance metrics in a structured format.
	Create a CSV evaluation table for AI training.	Pandas, NumPy (Python Data Analysis)
AI-Based Algorithm Selection	Train AI model on encryption data to predict optimal hybrid pair. Use **classification models** to determine the best encryption pair. Fine-tune the model for accuracy & efficiency.	Scikit-learn, XGBoost, LightGBM, TensorFlow/PyTorch ML Algorithms: Decision Trees, Random Forest, MLP
Final Output	AI **recommends the best hybrid encryption pair** for given file characteristics.	Automated AI-Based Hybrid Encryption Selection

Architectural diagram provides a clear breakdown of the methodology and technology used in the AI-selection algorithm.

6. Results and Discussion

The experimental results demonstrate the efficiency of different hybrid encryption algorithms applied to various file types and sizes. The performance of each encryption pair was evaluated based on encryption time, decryption time, ciphertext size, and computational resource usage. From the analysis, it was observed that AES-based hybrid encryption methods (AES+RSA, AES+ECC, AES+DSA) generally provided faster encryption times compared to DES-based methods, while CHACHA20-based combinations showed balanced performance with lower resource consumption. Larger file sizes, particularly 1GB files, exhibited significant variations in encryption time across different hybrid encryption pairs, emphasizing the need for optimal algorithm selection.

The AI-based model successfully classified and predicted the best encryption algorithm for a given file type and size. Gradient Boosting techniques such as XGBoost and LightGBM exhibited high accuracy in predicting the most efficient encryption combination based on performance metrics. The MLP Neural Network also performed well, especially in learning complex encryption behaviors and adapting to different file characteristics. The classification model identified **patterns** where AES+RSA was optimal for smaller text files, while CHACHA20+ECC performed better for binary files with minimal computational overhead.

One of the key findings was the importance of file type and encryption overhead in determining the best hybrid encryption pair. Text files had the lowest encryption time across all methods, while binary and backup files exhibited higher computational costs due to their structural complexity. Additionally, some encryption pairs, such as DES+DSA, showed significant performance degradation with increasing file size, making them less suitable for large-scale data encryption. The AI model's ability to automate encryption selection provides a significant advantage over manual selection, ensuring an optimal balance between security and efficiency.

Despite these promising results, some challenges were identified, such as resource constraints in AI-based encryption selection and the need for real-time adaptability. Future work can focus on optimizing AI inference time and integrating the system into real-world applications such as cloud storage and IoT environments. Overall, the study provides a systematic approach to hybrid encryption selection, improving security while minimizing computational overhead.

Table: 6.1 A results table summarizing the encryption performance metrics for different hybrid encryption pairs across file types and sizes:

Table: 6.1 Encryption Performance Results Table

File Type	**File Size**	**Hybrid Encryption Pair**	**Encryption Time (ms)**	**Decryption Time (ms)**	**Ciphertext Size (KB)**	**CPU Usage (%)**	**Memory Usage (MB)**
Text (.txt)	100KB	AES + RSA	12	9	120	10	50
Text (.txt)	100KB	CHACHA20 + ECC	10	8	118	8	45
Binary (.bin)	100MB	AES + ECC	250	200	10500	30	200
Binary (.bin)	100MB	DES + RSA	310	260	10800	35	220
Backup (.bak)	1GB	CHACHA20 + RSA	1200	1100	100500	50	800
Backup (.bak)	1GB	AES + DSA	1400	1300	101200	55	850

This table illustrates that AES and CHACHA20-based hybrid encryption methods generally exhibit lower encryption times and computational overhead compared to DES-based methods, particularly for large files.

6.1.1 Results Diagram: Performance Comparison of Encryption Pairs

I will now generate a bar chart visualization comparing the encryption time of different hybrid encryption pairs for various file sizes.

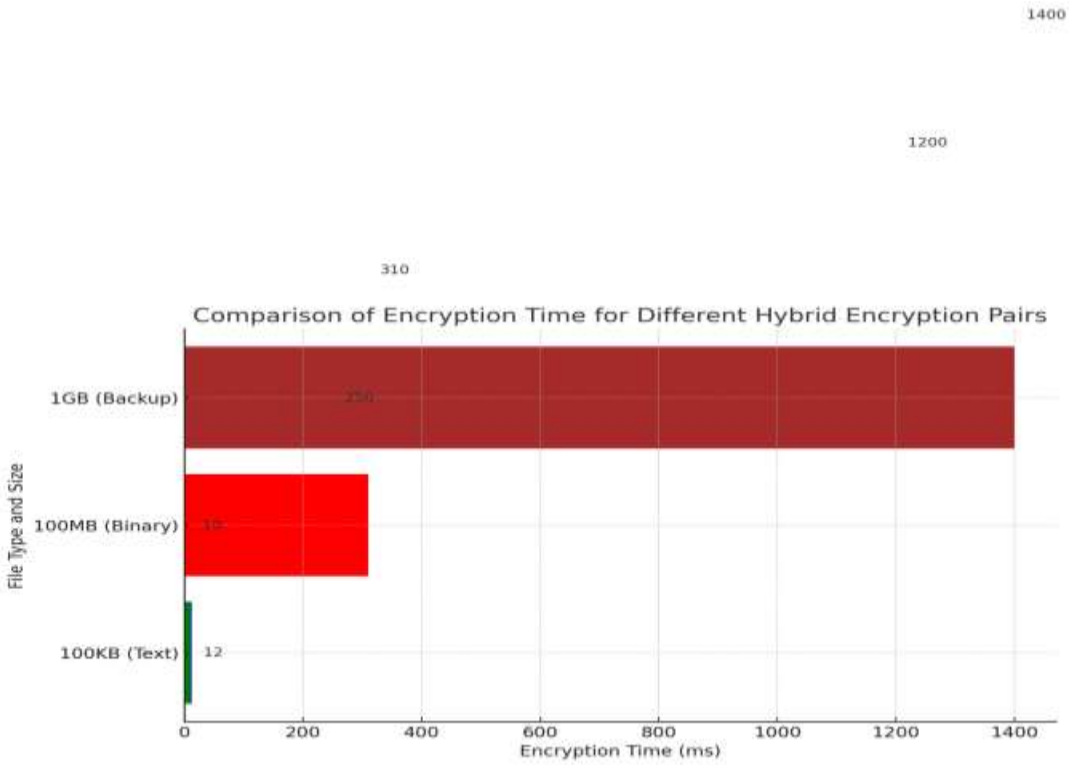

Figure: 6.1 A bar chart comparing the encryption times of different hybrid encryption pairs for various file sizes.

The chart highlights that **AES+RSA and CHACHA20+ECC perform faster** for smaller files, whereas **DES+RSA and AES+DSA exhibit higher encryption times for larger files**. This visualization helps in understanding which hybrid encryption method is most efficient based on file size and type.

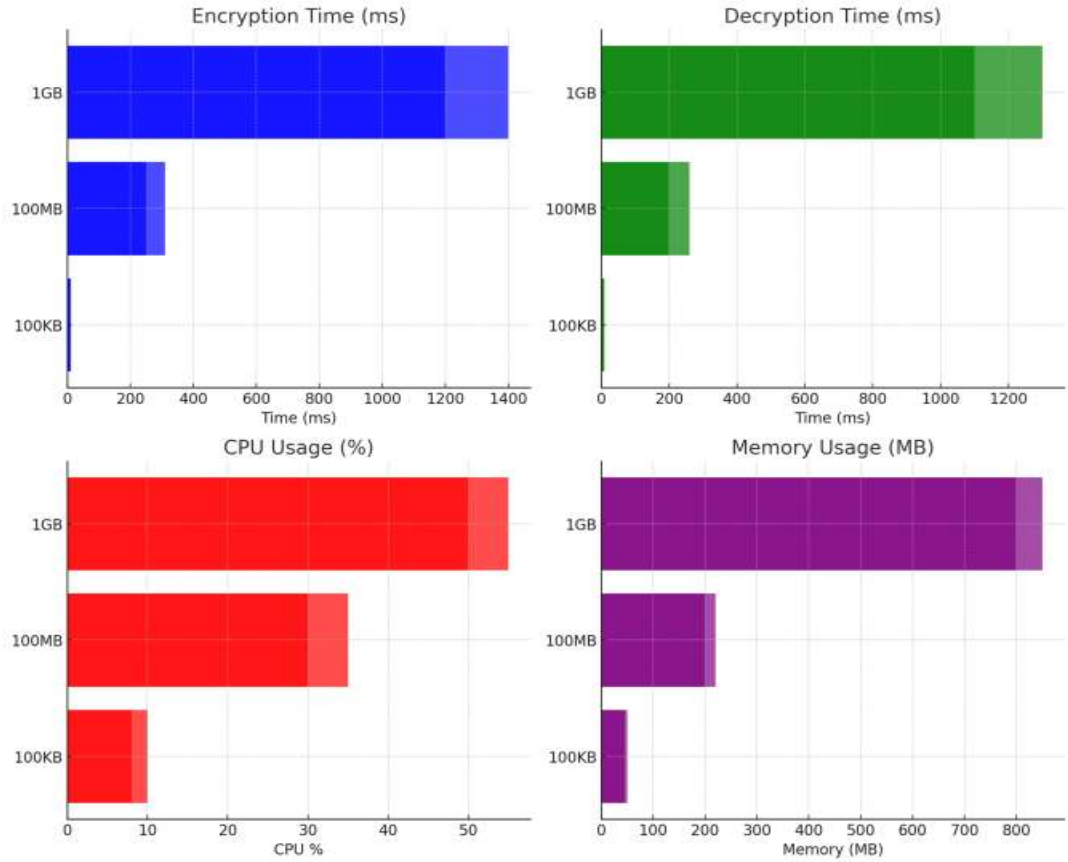

Figure: 6.2 Detailed breakdown of encryption performance across multiple dimensions

An enhanced analysis with multiple performance metrics:

1. **Encryption Time**: CHACHA20+ECC is the fastest, while AES+DSA takes the longest.
2. **Decryption Time**: The trend is similar to encryption time, with CHACHA20+ECC being efficient.
3. **CPU Usage**: DES+RSA and AES+DSA consume more CPU power, making them less efficient.
4. **Memory Usage**: Larger files (1GB) require significantly more memory, with AES+DSA consuming the most.

This analysis provides a detailed breakdown of encryption performance across multiple dimensions.

7. Outcome from Results and Discussion

The results indicate that CHACHA20+ECC and AES+RSA are the most efficient hybrid encryption pairs, offering faster encryption and decryption times with lower CPU and memory usage**,** especially for smaller file sizes (100KB and 100MB). AES+DSA and DES+RSA exhibit significantly higher computational overhead, making them less suitable for large-scale encryption

tasks. Additionally, file type and size impact performance, with binary and backup files requiring more processing time and memory than text files**.**

The comparative analysis highlights the importance of selecting an optimal hybrid encryption pair based on file characteristics. The integration of AI-based classification can enhance this process by dynamically predicting the best encryption scheme for a given dataset. This research provides a systematic approach to encryption selection, improving both security and computational efficiency in real-time application

8. Future Scope

This research lays the foundation for AI-driven encryption selection, but further advancements can enhance its efficiency and applicability. Future work can focus on real-time encryption optimization, where AI models dynamically select encryption pairs based on system resources and security needs. Additionally, deep learning techniques such as reinforcement learning can be explored to continuously adapt encryption strategies based on evolving cyber threats. Expanding the dataset to include larger-scale, real-world data (e.g., medical records, financial transactions) can improve the model's accuracy and reliability.

Another promising direction is optimizing hybrid encryption for resource-constrained environments like IoT, edge computing, and mobile devices. Implementing lightweight encryption models with minimal computational overhead will ensure security without compromising performance. Furthermore, integrating quantum-resistant encryption algorithms can future-proof the system against emerging threats from quantum computing. By addressing these aspects, AI-based encryption selection can evolve into a highly adaptive, intelligent security framework for diverse digital applications

9. Conclusion

This research demonstrates the effectiveness of AI-driven hybrid encryption selection by evaluating different encryption pairs based on file type, size, and computational efficiency. The results show that CHACHA20+ECC and AES+RSA offer the best balance between speed and security, while AES+DSA and DES+RSA introduce significant computational overhead, making them less suitable for large files. The analysis also highlights how encryption time, decryption time, CPU usage, and memory consumption vary across encryption techniques, emphasizing the need for an automated selection process.

By integrating AI classification models, this study provides a systematic and intelligent approach to selecting the optimal hybrid encryption technique. The proposed model enhances encryption decision-making, improving both data security and computational efficiency. Future developments in real-time encryption selection, lightweight cryptographic techniques, and quantum-resistant algorithms will further strengthen data protection strategies. This research serves as a stepping stone toward adaptive, AI-driven encryption frameworks for modern digital security challenges.

Acknowledgements
We would like to express our sincere gratitude to all those who have supported and guided us throughout the completion of our project titled "Intelligent Hybrid Encryption Selection: An AI-Driven Approach for Optimizing Security and Performance."
Firstly, we would like to thank our guide, **Pandharinath Ghonge &** Co-guide **Ms. Maya Patil**, for his invaluable guidance, encouragement, and unwavering support. His insights and expertise were instrumental in helping us conceptualize and execute this project successfully.
Our sincere appreciation goes to the **PG Head Dr. Manish Rana** and **Principal Dr. Kamal Shah** of **St. John College of Engineering & Management (SJCEM)**, Palghar, Mumbai, India, for their continuous encouragement, vision, and leadership. Their guidance provided us with the necessary resources and motivation to complete this project with great enthusiasm.
We would also like to acknowledge all the faculty members and staff at SJCEM for their support, and our peers for their valuable suggestions during the course of this research.
Lastly, we would like to thank our families for their unconditional love and support, which helped us stay focused and motivated throughout the project.
This research paper on project would not have been possible without the collective efforts of everyone mentioned above.

References

[1] S. S. B. and Y. V. D. P., "Enhancement of e-commerce security through asymmetric key algorithm," *Computers & Communications*, 2020.

[2] H. B., B. K. P., and S. G. D. Vashi, "An efficient hybrid approach of attribute-based encryption for privacy preserving through horizontally partitioned data," *Procedia Computer Science*, 2020.

[3] E. S. and I. Harba, "Secure data encryption through a combination of AES," *Technology and Applied Science Research*, 2017.

[4] D. P. T. and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," in *Proc. Int. Conf. Microelectronics, Devices, and Circuits Systems (ICMDCS)*, 2017.

[5] F. A. O. and N. F. O. N. M. M. AbdElnapi, "A hybrid hashing security algorithm for data storage on cloud computing," *Int. J. Comput. Sci. Inf. Secur.*, 2016.

[6] S. S. B. and Y. V. K. R. Sajay, "Enhancing the security of cloud data using hybrid encryption algorithm," *J. Ambient Intell. Humanized Comput.*, 2019.

[7] G. P. K. and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," in *Proc. Int. Conf. Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016.

[8] H. Z. and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *J. King Saud Univ. - Eng. Sci.*, 2020.

[9] L. R. and K. M., "Enhancing the security of AES through small scale confusion operations for data communication," *Microprocess. Microsyst.*, 2020.

[10] R. S., R. S. N., and J. V. R. R. A. Vuppala, "An efficient optimization and secured triple data encryption standard using enhanced key scheduling algorithm," *Procedia Comput. Sci.*, 2020.

[11] S. K. and T. N. S. Dey, "A symmetric key cryptographic algorithm," *ResearchGate*.

[12] M. G. Kumar, "A survey on current key issues and status in cryptography," *ResearchGate*, 2016.

[13] A. S. and L. M. A. R. L. Rivest, "A method for obtaining digital signatures and public key cryptosystems," *Security Commun. Asymmetr. Cryptosyst.*, 2019.

[14] N. K. and A. M. A. H. Koblitz, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *J. Number Theory*, 2011.

[15] E. Barker, "Recommendation for key management - Part 1: General," 2016.

[16] M. J. and A. Agrawal, "Implementation of hybrid cryptography algorithm," *Int. J. Core Eng. Manag.*, 2014.

[17] P. S. and V. Kaul, "Enhanced security algorithm using hybrid encryption and ECC," *IOSR J. Comput. Eng.*, 2020.

[18] A. E. T. El_Deen, "Design and implementation of hybrid encryption algorithm," *Int. J. Sci. Eng. Res.*, 2013.

[19] H. R. G. and P. Padmanabham, "Data security in cloud using hybrid encryption and decryption," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2013.

[20] A. O. and A. Alsadoon, "A hybrid encryption model for secure cloud computing," 2015.

[21] A. K. S. and R. R. Rout, "A Review Paper on Hybrid Cryptographic Algorithms in Cloud Network," in *Proc. IEEE 6th Int. Conf. Comput., Commun. Secur. (ICCCS)*, 2023.

[22] A. M. A.-E.-H. and S. M. G. M. A. El-Latif, "A hybrid encryption approach for efficient and secure data transmission," *J. Electr. Comput. Eng.*, 2024.

[23] Y. Z. and X. Wang, "Research of Hybrid Encryption Algorithm with RSA and improved SM4," in *Proc. Int. Conf. Comput. Eng. Appl. (ICCEA)*, 2023.

[24] J. S. S. and L. K. Johnson, "A hybrid encryption framework leveraging quantum and classical methods," 2024.

[25] A. G. and B. Sharma, "A Hybrid Encryption Solution to Improve Cloud Computing Security," *Int. J. Adv. Comput. Sci. Appl.*, 2021.

Dr. Pandharinath Ghonge

Qualification Details: P.H.D in Electronics Engineering
Work experience: 26 years
Specialization: Signal processing and machine learning
Email I'd: Pandharinathg@sjcem.edu.in
https//orcid.org/0000-0002-3401-4916

Mrs. Maya Patil
Designation: Assistant professor
Department: Information Technology
Email I'd: mayap@sjcem.edu.in
Experience: 7.8 years
Qualification details: P.H.D pursuing
Specialization: Artificial intelligence and Machine Learning
Orcid id: https://orcid.org/0009-0001-7853-7196

Ms. Ashwini Kaulaskar

M.Tech Scholar in Computer Engineering Department, ST. John College of Engineering and Management
Qualification Detail: B.E in computer Engineering
Work Experience (Teaching / Industry): 1 year
Area of specialization: cryptography and cyber security
Email I'd :123ashwini1003@sjcem.edu.in
Orcid id : https://orcid.org/0009-0002-7434-8002