iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83050

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

A New Hybrid Technique for Data Encryption In Distributed Computing Systems

Kajal Suresh Bagde[1], Prof.Bhagyashree Kumbhare[2], Prof. Yamini Laxane[3]
Smt. Radhikatai Pandav College of Engineering, Nagpur, India

***Abstract*—Distributed computing environments such as cloud computing, Internet of Things (IoT), edge computing, and distributed databases require secure and efficient data protection mechanisms. Traditional encryption methods often face challenges related to scalability, computational overhead, and secure key management. This paper proposes a hybrid encryption technique that combines Advanced Encryption Standard (AES) for fast data encryption, RSA/ECC for secure key exchange, and SHA-256 for data integrity and authentication. The proposed framework enhances confidentiality, integrity, and resistance against cyber threats including brute-force, replay, and man-in-the-middle attacks. Performance evaluation based on encryption time, decryption time, throughput, memory utilization, and security strength demonstrates improved efficiency and stronger security compared to conventional single-algorithm approaches. The proposed model provides a scalable, lightweight, and secure solution for next-generation distributed computing systems.**

***Keywords*—Hybrid Encryption, Distributed Computing, Cloud Computing, Internet of Things (IoT)**

I. INTRODUCTION

The quick development of distributed computing systems, such as cloud computing, big data platforms, and Internet of Things (IoT) settings, has completely changed how data is handled, stored, and sent via networks. Scalability, flexibility, and high performance are made possible by these systems' reliance on numerous linked nodes that work together to carry out computing operations. Distributed systems' decentralized structure, however, poses serious security risks, especially when it comes to maintaining data integrity, confidentiality, and safe node-to-node communication.

Protecting sensitive data against illegal access, interception, and cyberattacks is one of the main issues in distributed environments. Data is susceptible to dangers like eavesdropping, data breaches, and malicious intrusions since it is frequently sent over open or shared networks and kept in several locations. By transforming plaintext data into secure ciphertext that is only accessible by authorized users, encryption techniques play a critical role in reducing these dangers.

Symmetric and asymmetric cryptographic techniques are two main categories into which traditional encryption methods fall.

II. LITERATURE SURVEY

Over the last few decades, the Internet, computers, and With the growth of the information economy, mobile Internet technology has significantly altered human civilization and interpersonal communication. Our application requirements cannot be met by conventional computers without an Internet connection. The evolution of information exchange between objects is encouraged by ubiquitous connection. The Internet of things has been widely used in business, industry, organizations, education, national security, and everyday life in recent years.From the perspective of architecture, the Internet of things can be generally divided into three layers, namely perception layer, network layer, and application layer. The perception layer transforms the information of things to the readable digital signals via RFID, sensors, etc. On the other hand, the network layer transmits these digital signals to corresponding platforms via a connected network. In the end, the application layer unscrambles and applies digital signals through corresponding software. Among these three layers, security is a problem to ensure signal is corrected collected, transmitted, and interpreted by the applications. Both the ordinary nodes and sink nodes are vulnerable to a variety of security attacks, such as denial of service attacks, or illegal control and failure. These attacks could compromise the sensitive information and result in malfunctions. Therefore, information security has to be enforced for information integrity, confidently, and privacy.Encryption is a required step for the security of the Internet of things. The Advanced Encryption Standard (AES) and ECC (Elliptic Curve Cryptography) are broadly used for information security. It uses the elliptic curves as digital signature, and the speed of digital signature and authentication to faster than DSA(Digital Signature Algorithm), and AES algorithm encryption data is simple, fast and reliable. The hybrid key technology, which takes into account the characteristics of symmetric key and asymmetric key, is becoming more and more respected. But the application of the Internet of things is still in the exploration stage.

However, there are still issues on the encryption design when the encryption algorithm is applied to cheap devices of the Internet of things. Due to low computational resources, how to provide robust security with low computational complexity is challenging. In this paper, we address this issue and propose a mixed encryption algorithm to effectively use the heterogeneous capabilities of the networking components in the Internet of things systems. The sensor nodes can use the hardware encryption chip while the public key infrastructure PKI and password technology and other technical means ensure the security and safety for nodes to collect information. Our approach allows hybrid encryption to achieve a better effective on the information security while the information is transmitted over a number of networking components[1].Recently, Cloud computing is a new type of computing model for on demand network access to a shared pool of configurable computing resources that can be dynamically provisioned. The main motivation of thecloud computing is to provide scalable and low price on-demand computing infrastructures with fine quality of service levels. Many developers are struggling to make cloud-based applications secure for users. But it is not easy to provide real security with currently affordable technological abilities[2].A secure computing environment would not be complete without consideration of encryption technology. The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. The use of simple codes to protect information can be traced back to the fifth century BC. As time has progressed, the methods by which information is protected have become more complex and more secure. Encryption is a method of transforming data with the intension of keeping it a secret. uses an It algorithm called a cipher to encrypt data and it can be decrypted only using a special key. Encrypted information is known as cipher text and the process of obtaining the original information (plaintext) from the cipher text is known as decryption. Encryption is specially required when communicating over an untrusted medium such as internet, where information needs to be protected from other third parties. Modern encryption methods focus on developing encryption algorithms (ciphers) that are hard to break by an adversary due to the computational hardness (therefore could not be broken by a practical means). Two of the widely used encryption methods are Symmetric key encryption and Public-key encryption. In Symmetric key encryption, both the sender and the receiver share the same key used to encrypt the data. In Public-key encryption, two different but mathematically related keys are used. Even though both encoding and encryption are methods that transform data in to a different format, the goals tried to achieve by them are different. Encoding is done with the intension of increasing the usability of data in different systems and to reduce the space required for storage, while encryption is done to keep the data secret from third parties. Encoding is done using publicly available methods and it can be easily reversed. But encrypted data cannot be decrypted easily. It requires the possession of special piece of information called a key[3].Cloud computing presents a holistic approach to offering services by reorganizing diverse content developed for consumers based on individual needs. It is also crucial for next-generation cellular telecommunications, hacking, and social computation. Cloud storage substantially decreases customers' storage load and provides them access flexibility, making it one of the essential cloud computing. However, cloud data protection, transparency, and trust have emerged as critical issues affecting the viability of cloud services and perhaps impeding the advancement of 5G (Fifth Generation) and cyber systems. To begin with, putting data in the cloud raises the danger of data leakage and fraudulent activity. Second, cloud computing services are increasingly emerging targets of assaults and breaches, posing a threat to cloud data security. Database management activities in the cloud, such as information storage, restoration, migration, erasure, update, searching, querying, and accessibility, may not be fully trusted by their owners. Cloud providers should preferentially audit the dependability of data management[4].From their emergence, the two concepts of the Internet of Things (IoT) and cloud computing (CC) have evolved separately. For many years, they have seen independent evolution in their hardware and software aspects. In its evolution, IoT faces many problems among them storage capacity, energy efficiency, and computational capabilities. While looking for solutions to these problems, scientists found that CC could help to solve them. In addition, the Internet of Things could allow CC to handle real-world objects in a more dynamic way to deliver new attractive services and applications in some practical applications. Hence, the need to merge the Cloud and IoT technologies emerge. As a result, the concept of the Cloud of Things (CoT) was born. This integration is useful because the resulting system is more powerful, and intelligent and offers promising solutions to the users. However, CoT faces a large number of challenges such as security, privacy, reliability, scalability, heterogeneity, power consumption, standardization, and others[5].In the ever-evolving IT landscape, cloud data centers stand as giants of innovation, transforming the way we store, process and access data on a scale previously unimaginable. Their ubiquitous presence in our digital lives has ushered in an era of unparalleled convenience, accessibility, and efficiency. However, in the midst of this digital utopia, a looming specter looms – the great challenge of protecting sensitive data in cloud environments. The relentless advancement of technology has brought with it increased security concerns, and data protection has become a critical battleground across the vast expanses of cloud data centers. As we unlock the enormous potential of cloud computing, we are acutely aware of the vulnerabilities it presents.

The imperative to fortify data storage fortresses against malicious intrusions and data breaches has never been more prominent. Since the start of its operation, the Internet has seen several changes, some of which have altered how people live today because cloud computing offers consumers a wide range of facilities as a service, this new technology has swiftly gained popularity [6].Encryption and decryption are essential processes with the purpose of preserving data privacy and security. The process of converting plain text information onto cipher text which appears random and meaningless is known as encryption [1]. Decryption is the process of converting encrypted data from cipher text to plaintext, which is able to read and recognize. Symmetric key cryptography and asymmetric key cryptography are the two fundamental divisions of encryption: Symmetric key cryptography. In this method a single secret key is utilized for both the encryption and decryption of data. It is crucial that this key be kept confidential and only shared between the sender and receiver of a message[8].With the growth of big data, the need for secure and efficient data storage and transmission has become increasingly important. Traditional encryption algorithms, such as AES and RSA, provide good security for small data, but are not optimized for big data due to their high computational overhead and limited scalability. This has led to the development of new encryption algorithms that are specifically designed for big data security. The characteristics of big data, including volume, velocity, variety, veracity, venue, validity, vocabulary, vagueness, and value, make it challenging to store, process, and analyze using traditional methods. Big data analytics aims to extract insights and knowledge from these large and complex datasets, but this process is often hindered by security concerns, such as data breaches and unauthorized access. Hybrid encryption algorithms are a promising solution for big data security, as they combine the strengths of symmetric and asymmetric encryption to achieve both security and efficiency. In a hybrid encryption scheme, a symmetric encryption algorithm is used to encrypt the data, and the key used for the symmetric encryption is itself encrypted using an asymmetric encryption algorithm, such as RSA or Elliptic Curve Cryptography (ECC)[9].The internet service industry, encompassing areas like cloud computing, represents a rapidly evolving model for large-scale infrastructure . Cloud computing has emerged as a transformative force across multiple industries, fundamentally changing how businesses manage and process data . The cloud computing model and its distribution architecture are built upon the Internet. Its main goal is to store sensitive information quickly and securely. Cloud computing enables globalaccess to a centralized collection of resources, including servers, storage, networks, services, and applications, via the Internet from any location in the world . There are risks associated with cloud computing[10].

A. Understanding of hybrid Techniques for Data Encryption in Distributed Computing Systems

A hybrid encryption technique combines multiple cryptographic methods to improve:

- Security
- Speed
- Scalability
- Reliability
- Key management

In distributed computing systems such as cloud computing, edge computing, IoT networks, and distributed databases, hybrid encryption is widely used because a single encryption algorithm alone may not satisfy all requirements.

B. Applications

Distributed computing systems are widely used in modern technologies such as:

- Cloud computing
- Internet of Things (IoT)
- Edge computing
- Distributed databases
- Smart healthcare
- Military communication systems

C. Ethical considerations

A new hybrid encryption technique for distributed computing systems improves:

- Data confidentiality
- Integrity
- Authentication

- Secure communication

Although strong encryption provides major security advantages, ethical considerations are essential when designing and deploying such systems. Researchers must ensure that the proposed technique is used responsibly, legally, and fairly.

Ethical analysis is important in journal papers because encryption technologies directly affect:

- Privacy
- Human rights
- Cybersecurity
- National security
- digital trust.

1. Data Privacy and Confidentiality

Ethical Concern

The encryption system must protect sensitive user information from unauthorized access.

Examples:

- Personal data
- Financial information
- Medical records
- Government documents
- Ethical Responsibility
- Researchers should ensure:
- Strong encryption standards
- Secure key management
- Prevention of data leakage

III. IMPORTANCE OF ICIADAS IN ACADEMIC AND NATIONAL CONTEXT

The International Conference on AI-Driven Data Science for Autonomous Systems (ICIADAS) plays an important role in:

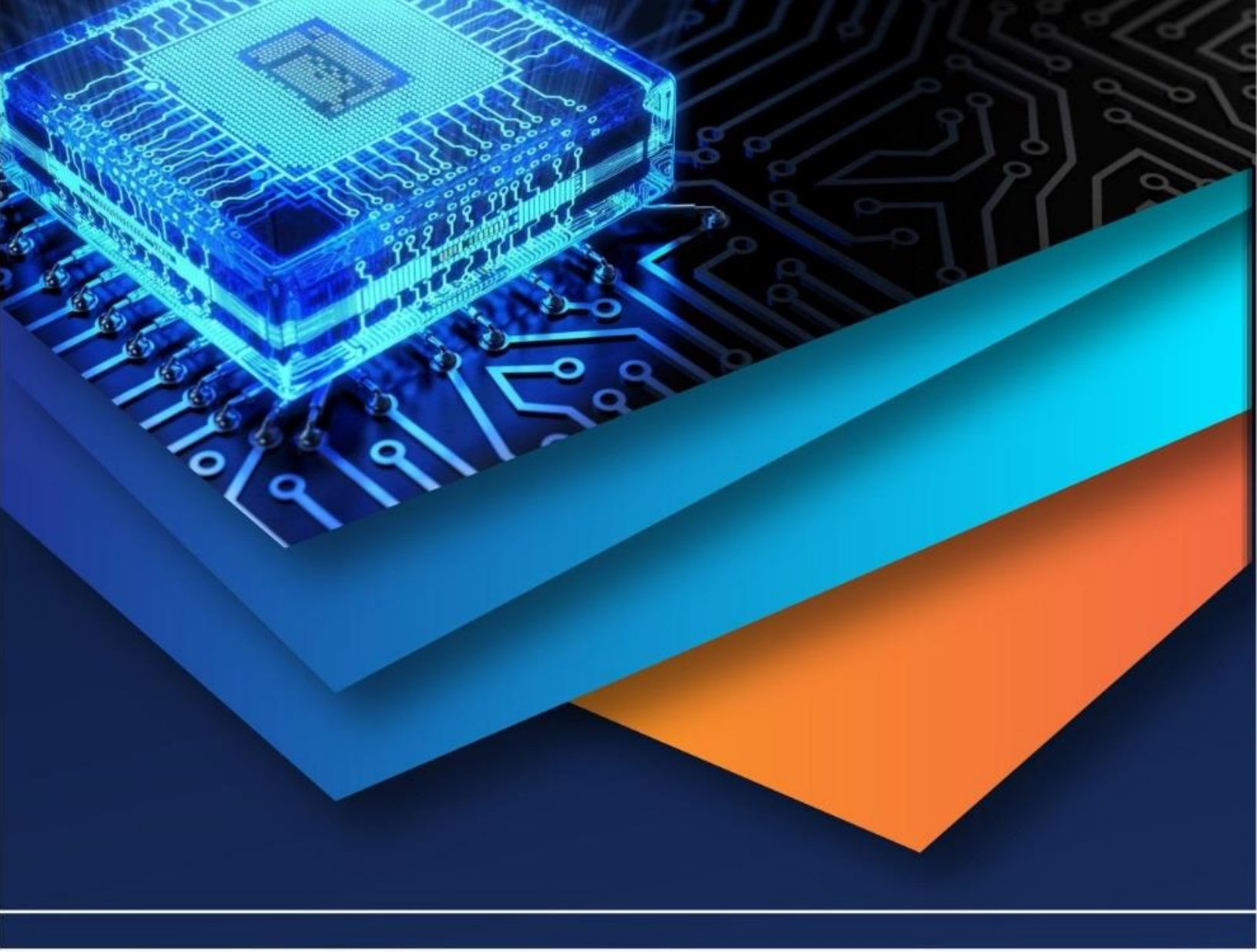
- Encouraging student research and innovation
- Promoting interdisciplinary learning
- Connecting colleges with industries
- Sharing real-world applications
- Discussing policies and ethical standards In a national and intercollege seminar, such a conference inspires young minds to explore research opportunities and contribute to technological advancement responsibly.

IV. CONCLUSION

A new hybrid technique for data encryption in distributed computing systems provides an efficient and secure solution for protecting sensitive information in modern digital environments. The proposed approach combines the strengths of symmetric encryption, asymmetric encryption, and hashing techniques to achieve improved confidentiality, integrity, authentication, and secure key management. By integrating fast data encryption methods such as AES with secure key exchange algorithms like RSA or ECC and integrity verification using SHA-256, the system overcomes many limitations of traditional single-layer encryption techniques.

The hybrid encryption model improves overall system performance by reducing computational complexity while maintaining strong protection against cyber threats including brute-force attacks, replay attacks, unauthorized access, and data tampering. The technique also enhances scalability and reliability in

distributed environments such as cloud computing, IoT networks, distributed databases, healthcare systems, banking applications, and edge computing platforms.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY