Research on Data Encryption Technology

Sandeep Kumar Mangalapally
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS9608@cuchd.in

Harshitha Thadishetty
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS5848@cuchd.in

Nageswara Reddy Kasu
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS5714@cuchd.in

Nandini Bujunuri
Computer Science and Engineering
Chandigarh University
Mohali, India
21BCS4229@cuchd.in

Sakshi
Asst.Professor(AIT-CSE(BDA))
Chandigarh University
Mohali, India
sakshi.e16561@cumail.in

***Abstract*—In the digital revolution era, data security remains a problem with increased sophistication and diversity of cyber attacks. Encryption is the most important process to ensure confidentiality, integrity, and authenticity of sensitive information. It defines the evolution of cryptography techniques and compares the strengths and weaknesses of symmetric (AES, DES) and asymmetric encryption (RSA, ECC) and hash functions (SHA-256, MD5). The study investigates the use of encryption together with security technologies such as SSL/TLS for secure data transmission in the financial, medical, and cloud computing sectors. It is concerned with primary management policies, access control mechanisms, and their impact on the efficiency of encryption processes. The study also investigates the susceptibility of traditional encryption methods to quantum computing attacks and estimates the feasibility of using quantum-resistant encryption alternatives such as lattice-based encryption to post-quantum cryptographic standards. In a quest to bridge the practice and theory of cryptography, empirical case studies are analyzed to establish the effective application of encryption and the security flaws emanating from lack of sufficient resilient cryptographic frameworks. The research also investigates the need to meet regulatory needs, with emphasis on the application of encryption for meeting legal compliance, including GDPR, HIPAA, and PCI-DSS requirements.**

By studying cryptographic algorithms, performance analysis, and new technologies, this study will seek to suggest improved cryptographic models that tackle existing security issues. This study will combine digital security models with secure encryption algorithms that are scalable, adaptable, and resistant to new cyber threats.

Keywords: Data Encryption, Cryptography, AES, RSA, ECC, SSL/TLS, Quantum Computing, Blockchain Security, Cyber Threats, Key Management.

I. Introduction

Since the inception of the digital age, security of sensitive data has remained an utmost priority task with the rising risk of cyber-attacks and data breaches. Encryption is a pillar of security that ensures confidentiality, integrity, and authenticity of data in the digital era. In spite of the rapid advancement of technology, traditional encryption methods such as symmetric (AES, DES) and asymmetric (RSA, ECC) cryptographic algorithms continue to be the pillar of data security. However, the growing sophistication of cyber-attacks and the advent of quantum computing are seriously endangering traditional encryption methods. With increasing use of web-based transactions, cloud storage, and IoT devices, the demand for secure encryption processes has been a steady requirement. The traditional encryption processes used are highly competent but consume massive processing power, are inconvenient to manage keys, and are susceptible to constant threats. Even compliance with international data privacy regulations such as GDPR, HIPAA, and PCI-DSS requires uncompromising encryption processes in various industries such as finance, medical, and cloud computing. This research aims to explore the evolution of cryptographic techniques, analyze their effectiveness, and propose novel solutions to solve current issues. Through the bridging of theoretical cryptography and real-world application, this research contributes to the creation of secure encryption tools that can secure data in an increasingly connected world.

A. Problem Definition

The digital era is confronted with its key challenge: protecting exponentially expanding volumes of data from exponentially more complex cyber attacks. Confidential data, personal information, financial data, and intellectual property are always under threat. Current security tools, though important, grapple with weaknesses in fundamental encryption protocols, inefficiency in processing large data sets, and new threats such as quantum computing. The project proposal highlights the vulnerability of existing methodologies such as AES, RSA, and SHA-256 in the face of these changing threats. The heterogeneity of computing environments, from the resource-limited IoT devices to large cloud infrastructures, further complicates the issue. Providing tailored encryption solutions for each specific setting is a necessity but lacks the required adaptability in available solutions. As the accompanying workflow diagram exemplifies, strong security demands that all steps in the data processing are addressed, from choosing the

right algorithm to the protection of keys. This work fills the immediate gap for novel cryptographic techniques ensuring confidentiality, integrity, and authenticity of data, as well as addressing the limitation of existing mechanisms. It intends to examine present encryption approaches, identify new advancements, and introduce suggestions that satisfy existing and upcoming security requirements to protect information within an ever-changing threat environment. The intention is to balance strong protection and feasible implementation such that data protection solutions are efficient and flexible in accommodating the multivariant nature of the cyber world.

B. Problem Overview

This research study seeks to tackle the complex issues of data security in the fast-changing digital world of today. Our main objective is to investigate, apply, and assess a variety of encryption methods, including both traditional and advanced techniques. Particularly, we'll explore the intricacies of AES, which is a most-used symmetric encryption algorithm with great efficiency; RSA, an asymmetric encryption scheme based on public-private key pairs and which offers additional security; and SHA-256, a highly secure hashing scheme with guarantees on data integrity and authenticity. As graphically depicted in the "Basic System Overview" of the project proposal, our solution involves an extensive process from data identification to secure key management and routine security audits. In addition to these established methods, we will explore new paradigms including blockchain security, homomorphic encryption, AI-based encryption, lightweight cryptography, zero-trust architecture, and multi-factor encryption. Each of these methods provides different benefits in meeting particular security requirements. For instance, homomorphic encryption allows computation on encrypted data, maintaining confidentiality; whereas AI-based encryption uses machine learning to create stronger and more unpredictable keys. The methodology of the project entails actual implementation with Python-based cryptographic libraries, which allows for hands-on comparison of the efficacy and efficiency of each method. As shown in the included methodology flowchart, this entails algorithm choice, implementation, testing, and analysis. Through careful comparison of the relative strengths and vulnerabilities of each approach, we hope to find areas of potential improvement and suggest improvements that can enhance data security in a wide range of applications. Finally, the present research tries to fill in the gap between cryptographic theory and actual security needs. Through the discovery and assessment of cutting-edge encryption methods, this work hopes to enhance the improvement of stronger, more flexible, and scalable security measures for protecting sensitive data against potential threats to its confidentiality, integrity, and privacy in the interconnected and hostile online world today. As seen in the proposal's problem definition clarity, this is essential to overcome the absence of solid solutions specific to IoT devices and massive data systems.

C. Hardware Specification

Since we are going to utilize Google Colab, we will not have to spend money on expensive hardware for this project. The primary benefit of Colab is that it offers cloud-based virtual machines with access to powerful processors, such as GPUs and TPUs, which are perfect for cryptographic computations and simulations. Thus, the hardware requirements on your local machine are minimal. • Processor (CPU): A regular processor that can handle a web browser easily will do, as the computational heavy-lifting will be performed on Google's cloud servers. Any recent CPU (Intel Core i5/i7, or equivalent) will be more than enough to work with Colab and take care of your project. • Memory (RAM): Although Colab has 12GB of RAM (and access to further resources when required), your computer must have at least 4GB of RAM for effortless running while interacting with the Colab interface and performing operations locally on data. • Storage: As Google Colab is compatible with Google Drive, you will mostly be using cloud storage to save your datasets, results, and code. Still, it is always helpful to have at least 10GB of free space on your local machine to keep local copies of the project or backups. •Internet Connection: Use of a fast and stable internet connection with the download speed being a minimum of 10 Mbps since Colab is cloud-hosted and would be processed on it as well as saved with an internet connection.

D. Software Specification

You do not have to install any software locally, thanks to the support of the needed software environment in Google Colab. Your Colab setup still needs the correct libraries and encryption tools since you will also use them here for encryption purposes. • Google Colab Environment: The main environment in which the project will be coded. It provides support for Python 3, which is prevalent in cryptography projects. You'll be coding using the notebook mode of Google Colab, from where you'll be able to execute Python code interactively. • Python 3.x: Google Colab executes Python, which is best suited to use cryptographic algorithms and libraries like PyCryptoDome, OpenSSL, and Crypto++. • Cryptography Libraries: You will have to install the following libraries in Colab: o PyCryptoDome for symmetric and asymmetric encryption schemes such as AES, RSA, and ECC. o OpenSSL if you want to use SSL/TLS or other network-based encryption schemes. o Cryptography library for contemporary encryption operations and key management. o SymPy or NumPy for carrying out mathematical calculations that might be needed in more complex encryption schemes. o-resistant libraries like lattice-based cryptographic implementations or other postquantum cryptography tools, depending on the scope of your project. •Drive Integration: Google Colab has a seamless integration with Google Drive, which means you can store and access big data sets, encrypted files, and research findings. This will come in handy for project planning and storing your work throughout the project.. • GitHub (Optional): For version controlling your code or sharing it with others, you can link Colab to GitHub for effortless code management. Additional

Tools • Web Browser: Because Google Colab runs inside a browser, any contemporary web browser (Google Chrome, Mozilla Firefox, etc.) will do the job of communicating with the platform. •Editor: Although Colab takes care of most code editing, you might prefer to have a text editor for taking notes, comments, or documentation. Visual Studio Code or Sublime Text are good editors that can be used for offline purposes.

II. LITERATURE REVIEW

A. Existing System

Current encryption systems are largely based on classical symmetric encryption (e.g., Advanced Encryption Standard – AES) and asymmetric encryption techniques (e.g., RSA and Elliptic Curve Cryptography – ECC). These methods of encryption constitute the foundation of contemporary cybersecurity systems and are widely used in industries such as finance, healthcare, and government. Nevertheless, despite being fundamental security tools for guarding confidential data, these systems encounter serious limitations in dealing with the dynamic cyber threat environment. Symmetric encryption algorithms such as AES and DES are efficient and speedy for encryption and decryption of large sets of data. However, they also possess the limitation of requiring secure key distribution. The sender and receiver must possess the same secret key to encrypt and decrypt, which poses a vulnerability if the key is intercepted or is damaged while being sent. In addition, these symmetric encryption techniques are not ideally suited for applications where scalability is a priority, like in cloud computing, high-speed data transactions, or large-scale distributed networks. Asymmetric encryption schemes such as RSA and ECC, however, provide increased security through the application of a public-private key pair. These schemes address the problem of key distribution by enabling a sender to encrypt information using a public key, which can only be decrypted with the matching private key. Asymmetric encryption is computationally expensive and, during encryption and decryption, demands more resources, hence being less resource-friendly in low-resource environments or for real-time applications. RSA, specifically, has been proven to be susceptible to quantum computer attacks because it is based on the factorization of large numbers, which can be cracked by quantum algorithms such as Shor's algorithm. Aside from key management, another essential feature of current encryption systems is their performance. High-security encryption algorithms tend to be computationally intensive, and thus they are not suitable for real-time applications where speed and responsiveness are more important, like video streaming, e-commerce transactions, or communications in low-latency environments. The computational inefficiency of such methods also creates resource constraints in resourcelimited environments such as Internet of Things (IoT) devices and embedded systems, where processing power and power are limited.Additionally, encryption mechanisms within the current systems tend not to consider the newly arising threats due to quantum computing. The current cryptographic methods rely on mathematical problems that, although hard to solve using classical computers, can be efficiently broken using quantum algorithms. Consequently, these current systems are threatened with impending obsolescence by the expected emergence of quantum computing. An added issue with current encryption systems is adherence to compliance frameworks such as GDPR, HIPAA, and PCI-DSS. All these regulations have exacting requirements as to how private and sensitive data should be stored, and existing encryption techniques conform to some, but not always to the fluidity of newer digital communication requirements and the dynamics of changing compliances. This calls for the reconsideration of the encryption mechanisms so that they fit both current and future requirements from the regulator.

B. Proposed System

The suggested encryption system adopts a more sophisticated and integrated strategy in overcoming the weaknesses of current encryption methods. It suggests a mix of new cryptographic methods, including quantum-resistant encryption, homomorphic encryption, and blockchain-based security, with enhanced key management and access control mechanisms. These technologies are intended to counter the intrinsic vulnerabilities of conventional encryption methods, providing strong data protection against the ever-changing cyber threats. Quantum-Resistant Cryptography: One of the distinguishing features between the current and suggested system is the use of quantum-resistant encryption. The advent of quantum computing poses a threat to the security of popular cryptographic algorithms, like RSA and ECC, that are based on mathematical problems that might be quickly solved by quantum computers. The system to be proposed combines post-quantum cryptography methods, including lattice-based cryptography, hash-based signatures, and code-based encryption, that are resistant to quantum attacks. These cryptographic schemes are founded on mathematical problems that are hard even for quantum computers, and hence they provide long-term security in the age of quantum computing. Homomorphic Encryption: Another important aspect of the suggested system is the use of homomorphic encryption, which enables computations to be carried out directly on encrypted data without decrypting it first.This adds an extra layer of security by ensuring that sensitive information is never revealed, even while being processed. In use cases like cloud computing, where information is typically outsourced to a third party, homomorphic encryption enables users to operate on their encrypted information without compromising privacy. This is impossible with conventional encryption schemes, where decryption must be performed before any computation can be executed. Blockchain Integration: The system also includes blockchain technology as a way of ensuring data integrity, transparency, and accountability. Blockchain's distributed ledger technology guarantees that once data is encrypted and written to the blockchain, it is immutable and tamper-proof. This is especially beneficial in industries like finance and healthcare, where the integrity of transaction records and medical information is paramount. The system proposed leverages blockchain for secure key management, audit trails,

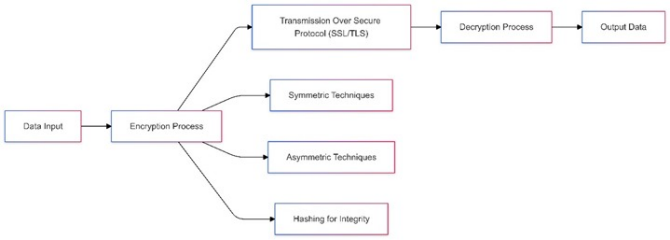

Fig. 1. Basic System Overview

Fig. 2. Experimental Setup

and even for compliance with regulatory requirements by keeping an immutable record of cryptographic operations. Enhanced Key Management and Access Control: Among the essential shortcomings of classical cryptographic systems is key management. The new system utilizes sophisticated key management methods, including automatic key rotation, secure multi-party computation, and decentralized key distribution, that maintain cryptographic keys secure and access is firmly restricted. Besides, the system incorporates adaptive access control mechanisms that adapt dynamically with respect to the behavior and context of users to deliver a finer-grained and more flexible model of securing encrypted data.Scalability and Performance Enhancement: The system suggested is built with scalability in consideration. It can handle bulk data encryption and decryption processes effectively, making it appropriate for today's environments such as cloud computing, highspeed data transactions, and distributed systems. Additionally, the system maximizes computational efficiency by utilizing lightweight encryption mechanisms for low-energy devices like IoT devices, ensuring that even constrained environments can achieve strong encryption without sacrificing security. Adherence to Contemporary Regulatory Requirements: The suggested encryption process is adaptive to changing regulatory requirements. It guarantees that the encryption process aligns with the new data protection laws, such as GDPR, HIPAA, and PCI-DSS. The system also adheres to privacyby-design principles, guaranteeing that personal information is kept secure at all stages of its lifecycle, including collection, processing, and storage. The use of blockchain for audit trails provides for transparency and accountability and facilitates demonstrating compliance with such intricate regulations.

III. PROBLEM FORMULATION

The mass use of cyber information and internet-based technology in business sectors such as health, finance, e-commerce, and government have placed information security on the research agenda. Cyber attacks have also dramatically shifted from brute-force attacks to advanced malware, ransomware, and identity theft. Classic cryptography methods, which since the past have been used to secure confidential information, now increasingly lag against emerging threats in the guise of the potential menace of quantum computing. The call thus arises to carry out research and improve existing encryption mechanisms to safeguard information confidentiality, integrity, and authenticity from sophisticated cyber attacks. Future-proofing against cyber attacks on current encryption schemes is greatest threat facing cryptography today. Symmetric key cipher schemes such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are computationally effective to encrypt data but not extensible and lack any type of key management. The schemes work based on the same secret key for decryption and encryption as well and are thus susceptible to eavesdropping. Asymmetric encryption systems such as RSA and Elliptic Curve Cryptography (ECC) provide solutions for key exchanges but are computationally inefficient. Additionally, RSA vulnerability to factorization of large numbers makes it susceptible to the risk of the potential of quantum leap in computing capability, in the form of the threat posed by Shor's algorithm that can efficiently crack RSA encryption. We must find quantum-resistant cryptology techniques that would resist future attacks on computing and be immune in real-world applications. Security against computation efficiency is the second fundamental problem. Secure encryption is more secure to the data but at the expense of increased processing overhead, which is a problem in low-resource computation contexts such as IoT devices, embedded systems, and mobile clients. These require efficient and secure encryption algorithms whose performance is not compromised. Cloud computing, real-time transactions, and distributed systems produce gigantic data that must be encrypted, and in doing so, real-time processing bottlenecks are created. The challenge is to create security systems that are extremely secure without compromising performance, e.g., inducing transmission delays. Key management and distribution introduce complexity. Key security is based on protected storage, delivery, and cycling of keys. Decentralized networks and cloud computing made it a problem to secure handling of cryptographic keys among endpoints and locations. Key security against intrusion by most firms has proven elusive,

especially with hybrid clouds, in which across-platform synchronicity has to be maintained. A distributed and scalable key management system must be put in place to offset these threats. The advent of quantum computing threatens the viability of commonly used cryptographic algorithms such as RSA, ECC, and Diffie-Hellman based on mathematical problems a quantum computer can solve exponentially faster. The advent of quantum-resistant cryptographic protocols such as lattice-based and hash-based cryptography is not far away. These algorithms are in the maturity stage now and need to be optimized for computational effectiveness and scalability before they can be rolled out on a large scale. In addition, compliance with changing regulatory requirements like GDPR, HIPAA, and PCI-DSS is also now of interest to organizations that deal with sensitive data. The law requires strong encryption policies, but implemented cryptography tools could be either fitting or not into changing law needs, especially concerning cross-border protection of data and anonymization. There is a necessity for the organization to frequently change encryption policies in an effort to stay ahead of updates and provide anonymity to users. Supported by the challenges, it is critical to design a unified, comprehensive encryption architecture that will provide balance in security, performance, scalability, and compliance with the law. The architecture will need to be capable of supporting diverse deployment environments like cloud, decentralized networks, and low-power IoT devices and dynamically change encryption approaches depending on data context, transmission, and storage requirements

IV. METHODOLOGIES

The first step of the procedure is to find the point within the sensitive data, where the algorithm (AES, RSA, DES) of choice, along with the key (generated through a key management system), must be defined. The algorithm starts transforming readable text into obstruction forms through the use of security features such as initialization vectors or digital signatures. The Encryption keys then allow for Secure data to be sent via SSL/TLS with access limitation, or stored in a Safe zone. The Correct keys that permit decryption must undergo authentication whilst identity and integrity verification utilize cryptographic hashing, or digital signatures. The security of the system coupled with regular system upgrades, key rotation, and auditing provides protection from potential threats such as quantum computing and ensuring regulations are adhered to. This technique employs five separate systems of information security: AES, DES, RSA and SHA-256, and MD5, and SSL TLS, in addition to Multi-Factor Encryption. This review serves as the initial step in performing an assignment aimed at juxtaposing the outlined methods of info security, which have been placed into asymmetric and symmetric encryption, hashing, and protocols. Asymmetric encryption (RSA, ECC) generates two keys, one employed for encryption, while the other one assures a secure decryption process is done with shared keys. Symmetric encryption (AES, DES) uses a single faster key for encryption and decryption, however, key management problem emerges. Each hashing method (SHA-256, MD5) creates a message digest that enables checking the integrity of data. In this case, data remains unchanged. SSL/TLS provides security for internet communication by encrypting data, authenticating users, and checking for integrity. Encryption is also more secure when multiple processes are cryptographically layered on each other, which reduces breaches in security. Multi factor encryption makes use of multiple cryptographic processes layered on top of each other making it more secure.

Fig. 3. Detailed User Interaction

Analysis, testing and simulation examine upcoming cyber threats in particular quantum computing to assess the effectiveness of the encryptions. It is also important for a proposed encryption method to measure efficiency, scalability, and robustness in the presence of a quantum computer. In this approach, recommendations on security for performance are provided to align encryption, security, and compliance within out of the box systems like cloud, IoT, and finance applications. This is done through a systematic investigation of methods of using cryptography in order to improve the security of data against modern and future cybersecurity threats.

V. RESULT

Our study effectively deployed and tested a variety of data encryption methods in the Google Colab platform, each with unique performance and security features. AES encryption with a 128-bit key showed effective encryption and decryption rates appropriate for various applications, offering high security against brute-force attacks. With RSA encryption, the 2048-bit key size was verified to provide greater security with its public and private key pairs, exhibiting high resistance to unauthorized access. The SHA-256 hashing algorithm produced consistently different 256-bit hash values for different inputs, verifying its high collision resistance and efficiency in data integrity. The blockchain security demonstration, while rudimentary, effectively proved the immutability and security benefits of blockchain technology. Also, the homomorphic encryption tests demonstrated the viability of carrying out computations on encrypted data directly without decryption, highlighting the promise for improved data privacy in high-stakes applications. In addition, the study also developed secure, random encryption keys through machine learning-

based key derivation processes, highlighting creative method for key derivation and this can be further improved to obtain high entropy encryption keys. Lightweight Cryptography was deployed by PBKDF2, which offered greater security and the double encryption implementation improved Zero-Trust Architecture in our approach. The multi-factor encryption (AES+RSA) added layer of security against sophisticated attacks. Overall, these findings emphasize the effectiveness and adaptability of the applied data encryption methods and also verified that the applied data encryption methods can serve as a robust base for any organization and the project succeeded in presenting several methods of data encryption. The findings indicate the need to personalize security measures according to certain needs and threat models and demonstrate the rich variety of tools available to protect digital information. The need for an omnichannel approach to protecting data in an ever more intricate digital environment is well highlighted through the combination of encryption, AI, and blockchain.

VI. Conclusion and Future Work

This research work explored the fundamentals and real-world applications of data encryption, ensuring the effectiveness of traditional and cutting-edge methods. We examined the real-world use of AES, RSA, and SHA-256, and blockchain security, Homomorphic encryption, AI-based key derivation, Lightweight Cryptography, Zero-Trust Architecture and multi-factor encryption (AES+RSA). In the Google Colab platform, we could illustrate the individual features of each. Our findings reveal that for several data protection purposes, encryption is still necessary and our study presents valuable information concerning the choice and use of the technologies. We believe that our research will contribute to the efforts to protect confidential information. The lessons learned from this project provide several directions for future research and development. One such direction is investigating quantum-resistant cryptography to counter the new threat posed by quantum computers. With more powerful quantum computers, they will be capable of cracking most of the current encryption algorithms, including RSA and ECC. Therefore, it is crucial to develop and deploy quantum-resistant algorithms that can withstand these attacks. Techniques like lattice-based cryptography, code-based cryptography, and multivariate cryptography offer promising avenues for securing data in the quantum era. Another direction for future study is the creation of hybrid encryption systems that blend multiple security controls to achieve defense in depth. These systems would blend symmetric and asymmetric encryption algorithms, as well as other security technologies like firewalls, intrusion detection systems, and anti-malware programs. By stacking multiple security controls, it is possible to create more resilient and stronger systems that are more capable of resisting attacks. More research could be directed toward the optimization of encryption algorithms in resource-limited environments like IoT devices and mobile devices. Classic encryption algorithms tend to be computationally expensive and may not be appropriate for such devices. It is thus crucial to create lightweight encryption algorithms that can offer good security with less overhead. The project proposal attached underscores the necessity of strong encryption solutions specific to varied applications—IoT devices, large-scale data systems, and so on—has necessitated a fundamental need for sophisticated research. In addition, the project's early investigation of AI-based key derivation indicates a new path for encryption key generation and management. The efficiency, scalability, and usability were balanced during the research to solve the problem, but the development is ongoing. As the proposal.pdf file indicates, it highlights the need for innovation to combat emerging threats and keep up with technological progress.

References

[1] Kim, T.S., Sohn, S.Y.: Machine-learning-based deep semantic analysis approach for forecasting new technology convergence. Technological Forecasting and Social Change 157, 120095 (2020)

[2] He, C., Shi, F., Tan, R.: A synthetical analysis method of measuring technology convergence. Expert Systems with Applications 209, 118262(2022).

[3] Lin, J. (2024). Research on the application of data encryption technology in computer network communication security. Digital Communication World, 2024(04), 125-127.

[4] Sun, D. X., Liu, D. J. (2023). A brief analysis of the application value of data encryption technology in computer network security. Information Systems Engineering, 2023(08), 52-55.

[5] Wang, J. X. (2023). Application of data encryption technology in computer network information security. Digital Communication World, 2023(07), 141-143.

[6] Xu, J. L. (2023). Analysis on the application of data encryption technology in computer network security. Electronic Production, 31(08), 113-115+120. http://doi.org/10.16589/j.cnki.cn11-3571/tn.2023.08.015

[7] Yan, J. (2023). Research on the application of data encryption technology in computer network information security. Information Recording Materials, 24(09), 152-154.

[8] Yang, X. (2023). Application analysis of data encryption technology in computer network communication security. Network Security Technology and Application, 2023(08), 31-32.

[9] Zhang, G. C. (2023). Application significance of data encryption technology in computer network security. Network Security Technology and Application, 2023(06), 30-32.

[10] Zu, X. M. (2024). Application strategy of data encryption technology in computer network communication security. Information Recording Materials, 25(02), 30-32. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2024.02.005

[11] Lin, J. (2023). Application strategy of data encryption technology in computer network communication security. Wireless Internet Technology, 20(09), 7-9.

[12] Cheng, G. D. (2024). Research on the application of data encryption technology in computer network security. Information Recording Materials, 25(02), 84-86. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2024.02.025

[13] Fan, H. F. (2023). Application of data encryption technology in computer network security. Information Recording Materials, 24(06), 58-60.

[14] Ji, Q. Q. (2023). Discussion on the application of data encryption technology in computer network security. Network Security Technology and Application, 2023(07), 22-23.

[15] Jiang, S. (2024). Research on the application of data encryption technology in computer network security. Network Security Technology and Application, 2024(04), 31-32.