INTERNATIONAL CONFERENCE ON RESEARCHES IN ENGINEERING, SCIENCE, TECHNOLOGY, MANAGEMENT AND HUMANITIES (ICRESTMH – 2024)

25TH AUGUST, 2024

CERTIFICATE NO : ICRESTMH /2024/C0824853

A Study to Secure Patient Data in E-Health Cloud Systems Through A Hybrid Cryptographic Method

Aparna Datta

Research Scholar, Department of Computer Science & Engineering,
Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

This study focuses on improving the security of patient data stored in e-health cloud systems. As digital healthcare becomes more common, protecting sensitive medical information is increasingly important. The research proposes a hybrid cryptographic method that combines multiple encryption techniques to provide stronger data protection. By using this approach, patient information remains safe from unauthorized access while still being accessible to authorized users. The study demonstrates how this method can enhance privacy, ensure data integrity, and support secure communication in cloud-based healthcare environments. Data security for electronic health record (EHR) applications in the cloud can be enhanced using the Password-Based Key Derivation Function (PBKDF2) in conjunction with Secure Hash Fixed-Based Output Cryptographic Algorithms (SHA-512). Attacks like Brute Force, Rainbow, and Man in the Middle are among the most prevalent forms of user aggressiveness that these technologies detect. Lastly, the execution time, memory space, and CPU time of each cryptographic hash technique were compared.

Keywords: *E-Health Cloud Systems, Patient Data Security, Hybrid Cryptography, Symmetric Encryption, Asymmetric Encryption.*

I. INTRODUCTION

In recent years, the rapid advancement of information and communication technologies (ICTs) has revolutionized the healthcare sector, paving the way for the widespread adoption of e-health systems. These systems, which integrate medical services, patient records, diagnostic imaging, and clinical decision support into digital frameworks, have enabled healthcare providers to deliver more efficient, accessible, and patient-centric care. The emergence of cloud computing as a fundamental backbone for storing and processing medical data has further accelerated the transition from traditional paper-based records to fully electronic health records (EHRs) and personal health records (PHRs). Cloud-based e-health platforms offer unprecedented advantages in terms of scalability, cost-efficiency, interoperability, and ubiquitous access, empowering healthcare institutions to share, retrieve, and analyze patient information across geographical boundaries. However, despite their transformative potential, e-health cloud systems face persistent challenges related to data security, privacy preservation, and regulatory compliance. The highly sensitive nature of medical records, coupled

with the legal and ethical obligations of safeguarding patient confidentiality, makes security a paramount concern. Any breach, unauthorized access, or malicious manipulation of healthcare data can not only compromise individual privacy but also lead to severe financial, reputational, and legal repercussions for healthcare providers.

Patient data stored in cloud environments is vulnerable to a wide range of cyber threats, including data interception, unauthorized disclosure, identity theft, ransomware attacks, and insider misuse. The distributed architecture of cloud systems, where data is stored across multiple remote servers operated by third-party service providers, inherently increases the attack surface. In addition, the multi-tenancy feature of cloud computing, where multiple users share the same physical resources, poses further risks of data leakage and side-channel attacks. Moreover, the dynamic nature of healthcare workflows often requires rapid access to patient data by multiple authorized entities, such as doctors, nurses, insurance providers, and researchers, further complicating the enforcement of strict security controls without hindering usability. These challenges necessitate the implementation of robust, efficient, and scalable security mechanisms tailored to the unique requirements of e-health systems.

Traditional security mechanisms, such as simple password-based authentication or basic encryption, are increasingly inadequate in mitigating sophisticated cyber threats targeting healthcare infrastructures. While conventional symmetric and asymmetric encryption methods have been employed to protect patient data in transit and at rest, each has inherent limitations. Symmetric key cryptography, for example, offers high-speed encryption but suffers from secure key distribution challenges, especially in large-scale and distributed cloud environments. On the other hand, asymmetric key cryptography, which uses public-private key pairs for secure communication, alleviates key distribution issues but is computationally more intensive, making it less efficient for encrypting large datasets such as high-resolution medical images or genomic data. In e-health systems, where both speed and security are critical, reliance on a single cryptographic approach may fail to meet the dual demands of performance and resilience against evolving cyberattacks.

The concept of hybrid cryptographic methods has emerged as a promising solution to overcome the limitations of individual encryption schemes. Hybrid cryptography strategically combines the strengths of both symmetric and asymmetric techniques to provide a balanced security-performance trade-off. Typically, the approach involves using asymmetric encryption to securely exchange symmetric keys, which are then employed for bulk data encryption. This layered methodology not only ensures the secure transmission of encryption keys over untrusted networks but also facilitates high-speed processing of large volumes of data. In the context of e-health cloud systems, such an approach can be instrumental in safeguarding patient data throughout its lifecycle—during transmission between healthcare providers, storage in cloud repositories, and retrieval for clinical or research purposes. By integrating hybrid cryptographic techniques, healthcare organizations can achieve enhanced confidentiality, integrity, and availability of medical records without compromising on operational efficiency.

In addition to technical performance, the adoption of robust cryptographic mechanisms in e-health systems must also align with regulatory and ethical frameworks governing the handling of medical information. Legislation such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and similar data protection laws in other jurisdictions mandate strict security controls for processing and storing patient data. Compliance with these regulations necessitates not only strong encryption but also secure key management, access control, audit logging, and incident response measures. Hybrid cryptographic methods, when designed and implemented effectively, can support regulatory compliance by ensuring that patient data remains inaccessible to unauthorized parties, even if the underlying storage infrastructure is compromised. Furthermore, with the growing integration of telemedicine, wearable health monitoring devices, and Internet of Medical Things (IoMT) ecosystems, the scope of patient data protection extends beyond centralized hospital systems to include a multitude of interconnected devices and endpoints. This further underscore the importance of versatile and adaptive security mechanisms capable of functioning seamlessly in diverse operational contexts.

E-Health Cloud Systems

E-health cloud systems represent the convergence of healthcare informatics and cloud computing technologies, offering a transformative approach to the storage, processing, and management of medical information in the digital era. At their core, e-health cloud systems integrate the capabilities of electronic health records (EHRs), personal health records (PHRs), telemedicine platforms, clinical decision support systems (CDSS), and Internet of Medical Things (IoMT) devices into a unified, scalable, and remotely accessible infrastructure hosted on cloud platforms. This paradigm shift from traditional on-premises data storage to cloud-based environments is driven by the need for interoperability, cost efficiency, scalability, and ubiquitous access to healthcare data. Unlike conventional systems where patient data is siloed within individual healthcare facilities, e-health cloud systems enable secure data sharing across geographically distributed medical institutions, allowing physicians, specialists, laboratories, insurance providers, and even patients themselves to access relevant information in real time. This not only enhances coordination of care but also reduces duplication of tests, facilitates faster diagnosis, and improves overall healthcare outcomes. The deployment models of e-health cloud systems—public, private, hybrid, and community clouds—offer varying degrees of control, customization, and cost-effectiveness, enabling healthcare organizations to select the configuration that best aligns with their operational needs and regulatory obligations. Public clouds, managed by third-party providers, offer high scalability and cost benefits but may raise concerns about data control and compliance, while private clouds provide greater security and customization at higher operational costs. Hybrid clouds combine the strengths of both, supporting sensitive data processing in private environments while leveraging public cloud resources for less critical workloads. Community clouds, designed for multiple organizations with shared goals, such as regional healthcare networks, facilitate collaboration while distributing infrastructure costs.

The adoption of e-health cloud systems is fueled by the growing volume, velocity, and variety of healthcare data, which includes structured clinical data, unstructured medical notes, diagnostic imaging, genomic data, and real-time patient monitoring streams from wearable and implantable devices. Traditional data management infrastructures often struggle to store and process such diverse datasets efficiently, whereas cloud systems provide elastic storage capacity and on-demand computational power to handle dynamic workloads. Furthermore, advanced analytics, artificial intelligence (AI), and machine learning (ML) algorithms integrated into e-health cloud platforms enable predictive modeling, personalized medicine, and population health management, thereby transforming raw data into actionable insights. For example, cloud-based AI models can analyze historical patient data to predict disease risk, optimize treatment plans, and identify potential adverse drug reactions, all in real time. Similarly, telemedicine services supported by cloud infrastructure allow healthcare providers to conduct remote consultations, monitor chronic conditions, and deliver follow-up care without requiring patients to travel to medical facilities, which is particularly valuable for rural or underserved populations. The flexibility of cloud-based systems also supports disaster recovery and business continuity, as data can be replicated across multiple geographical regions, ensuring availability even in the event of local system failures or natural disasters.

However, despite these advantages, the migration of sensitive patient data to cloud environments introduces significant security, privacy, and compliance challenges. Healthcare data is considered highly sensitive and subject to strict regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in Europe, and other regional privacy laws worldwide. These regulations mandate that patient data must be protected against unauthorized access, alteration, disclosure, and destruction. Cloud systems, by their very nature, involve data being stored and processed on remote servers owned and operated by third-party providers, which raises concerns over data sovereignty, control, and jurisdiction. The multi-tenancy feature of public cloud models, where multiple organizations share the same physical infrastructure, further heightens the risk of data leakage, side-channel attacks, and malicious insider activities. Additionally, the transmission of patient data over the internet exposes it to interception, man-in-the-middle attacks, and other cyber threats unless robust encryption and authentication measures are implemented. The growing sophistication of cyberattacks targeting healthcare—ransomware campaigns, advanced persistent threats (APTs), and supply chain compromises—demonstrates the urgent need for advanced, multilayered security frameworks in e-health cloud systems.

Addressing these challenges requires a comprehensive security strategy that combines technical safeguards, administrative controls, and policy enforcement. Encryption is a fundamental technical safeguard, ensuring that patient data remains unreadable to unauthorized parties both at rest in cloud storage and in transit across networks. Access control mechanisms, such as role-based access control (RBAC) and multi-factor authentication (MFA), help ensure that only authorized individuals can view or modify patient information. Audit logs and continuous monitoring provide traceability and

facilitate incident detection and response. Secure key management practices are critical in maintaining the integrity of cryptographic protections, especially in large-scale distributed environments where key distribution and revocation can become complex. For enhanced resilience, hybrid cryptographic methods, combining symmetric and asymmetric encryption, are gaining attention in e-health cloud security, as they offer both performance and strong key protection. Beyond technology, adherence to standardized frameworks such as ISO/IEC 27001 for information security management and ISO/IEC 27799 for health informatics security can guide healthcare organizations in building compliant and trustworthy cloud infrastructures. From a functional perspective, e-health cloud systems must not only safeguard data but also maintain high availability and low latency to meet the operational demands of healthcare delivery. A physician accessing a patient's electronic health record during a surgical procedure cannot afford delays due to network congestion or system downtime.

Consequently, cloud service providers supporting healthcare workloads must implement robust quality-of-service (QoS) guarantees, including load balancing, fault tolerance, and real-time synchronization across distributed data centers. Scalability is equally critical, as patient data volume is projected to grow exponentially due to advances in precision medicine, high-resolution imaging, and IoMT integration. Elastic scaling—dynamically allocating resources in response to demand—ensures that healthcare applications maintain performance under varying loads without incurring unnecessary costs.

II. REVIEW OF LITERATURE

Dutta, Aritra et al., (2023) Due to the multi-source nature of data and its transit via the internet, data security is an essential problem in cloud computing. Secure data is encrypted to prevent unauthorized access, yet brute force techniques may decrypt even the most well-protected files. We presented a strategy that integrates many algorithms—including Advanced Encryption Standard, proxy re-encryption, Honey, and N-th degree Truncated Polynomial Ring Unit (NTRU) or Number Theory Research Unit—to enhance data privacy and authentication. One well-known symmetric encryption approach that uses a secret key to both encrypt and decode data is Advanced Encryption Standard (AES). An intermediary may change the key used to encrypt a cipher text without having access to the plaintext by using the cryptographic method known as proxy re-encryption. One novel approach to message encryption is honey encryption, which makes it harder for attackers to tell the difference between genuine and fraudulent decrypted communications by inserting seemingly legitimate data into encrypted ones. The NTRU cryptosystem relies on the polynomial ring's public key. Data security for cloud-based outsourcing may be enhanced with the suggested method's combination of these strategies. Combining Honey and Hybrid cryptography makes it harder for unauthorized users to decipher signals that seem to be real. All things considered, these methods increase data security, safeguard user information, and guarantee that no one other than authorized users may access or change data kept in the cloud.

Boumezbeur, Insaf et al., (2022) The healthcare industry is one of several that has begun to see the value of cloud computing in recent years. Cloud computing makes it possible for medical providers to have 24/7 access to their patients' medical records, allowing them to better serve their patients. When medical records are kept on the cloud, they open themselves up to several forms of cyberattacks, including data loss, DoS, DDoS, and others. The public nature of cloud computing makes protecting sensitive information, such as health records, more of a challenge. Many issues could arise for a patient whose personal information is taken. These are problems that call for heightened safety measures. There is always the risk of hacking when sending sensitive information over the internet. Consequently, protecting the confidentiality of patients' information is a top priority for healthcare providers. A solution to this challenge is the adoption of encryption technologies that prioritize data security in the cloud to protect sensitive health information. In this research, we use a hybrid cryptography strategy to guarantee the safe transfer of health records to the cloud. Using a hybrid cryptography system, data is securely stored and transferred to and from the cloud, ensuring privacy and secrecy. The encryption key is split in half, allowing for controlled access to patient records using a specialized mechanism, which protects data from malicious insiders. This document serves as a functional system prototype that demonstrates the proposal's implementation and performance assessment. Time taken to generate keys, encrypt and decrypt records, upload and download records, and handle file sizes ranging from 0.1 MB to 500 MB are the metrics used for assessment. Conclusions The concept outperforms competing state-of-the-art solutions and demonstrates the feasibility of securely exchanging health data in the cloud.

Elamir, Mona et al., (2021) DNA computing draws inspiration from molecular biology and is a subfield of natural computing. It can decode data stored in DNA strands and do mathematical and logical operations on them. All patients, no matter where they are or what time of day it is, may benefit from E-health care services because to the fast advancement of network technology. Through a public channel, patients may access these services. Therefore, one of the most important concerns with E-health is the protection of patients' privacy. Using the Least Significant Bit algorithm—which entails concealing data in the least bit of picture pixels—this article proposes an encryption method for obfuscating patient information in medical images.

III. EXPERIMENTAL SETUP

The data is encoded into a DNA format after the picture is compressed using a key that is produced by a six-stage process using chaotic maps and DNA encoding rules. Six distinct medical pictures, including X-ray, CT, and MRI scans, were subjected to the suggested security system's examination. Various assessment measures have been used to assess the outcomes. It seems like the suggested plan is solid.

Using this web-based electronic healthcare administration system, staff, doctors, and patients may all be efficiently and pleasantly tended to. In addition to fixing the problems with the existing healthcare management system, the suggested approach also makes any healthcare institution a better place to work.

Built on wireless sensor networks, mobile phones, laptops, desktops, and other smart devices, this system allows for the real-time study of a plethora of patient variables. The plan is to build a set of modules that can track patients' data online and help physicians make more accurate diagnoses.

Caregivers and attendants may keep an eye on the patient at all times in case of an emergency. Thanks to the information gathered from the server, doctors and nurses can keep tabs on the patient at all times.

For easy access and processing in the event of logistical or possible problems, all of a patient's medical records, including prescriptions and reports, are stored in the cloud.

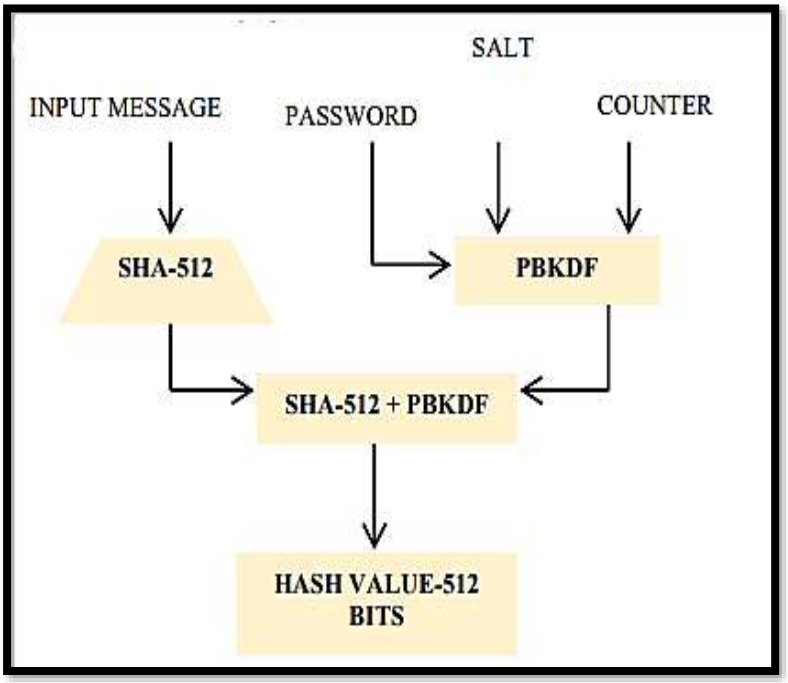

Figure 1: Block diagram of SHA-512 with PBKDF2

Several patients at public and private healthcare institutions, as well as one patient at home, may be tracked using this system. Using mobile phones to send data via the internet reduces the system's total cost.

We advocated for the use of the secure hash algorithm SHA-512 in conjunction with Passwordbased-KDF2 to provide patients and their families with access to cloud storage while also addressing the system's potential risks and privacy concerns.

IV. RESULTS AND DISCUSSION

There has been constant strife around cloud computing infrastructure development from the start. It finds that systems that assign security texture after the design has been submitted are less important than resilient, secure, and fault-prone systems.

Both SHA-1 and SHA-2 offers the secure hashing algorithms of 256 bits, 384 bits, and 512 bits. The output and execution results of several SHA algorithms using PBKDF2 are shown in the table and figures below.

Table 1: Performance Comparison of Various SHA Algorithms Using Input 'abc' (CPU Time, Memory Usage, Execution Time in ns & ms)"

Message / Password: abc	SHA-1	SHA-256	SHA-384	SHA-512+PBKDF2
CPU Time (Sec)	0.12	0.15	0.10	0.13
Memory	37532	37532	37680	37644
Execution Time (ms)	76.506113	67.248105	1.429335	76.328329

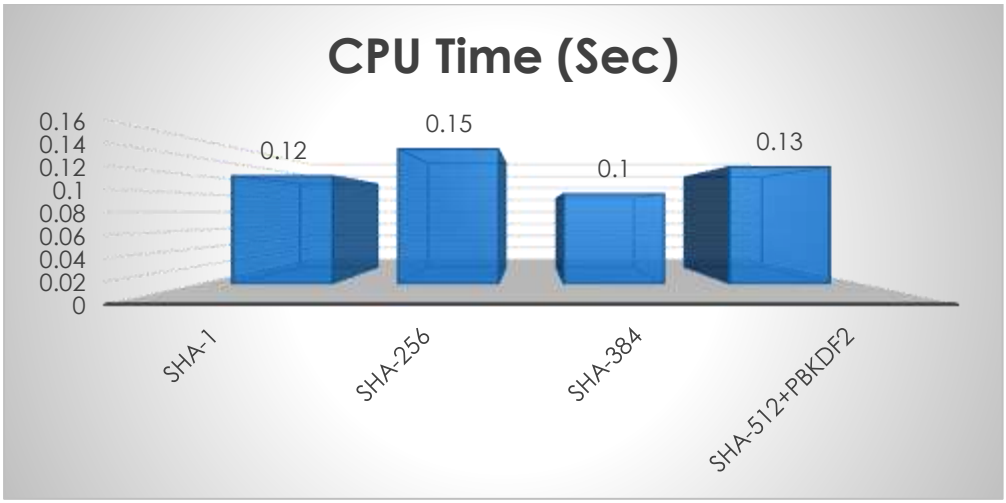

Figure 2: Comparison of CPU Time for Different SHA Algorithms with Input "abc"

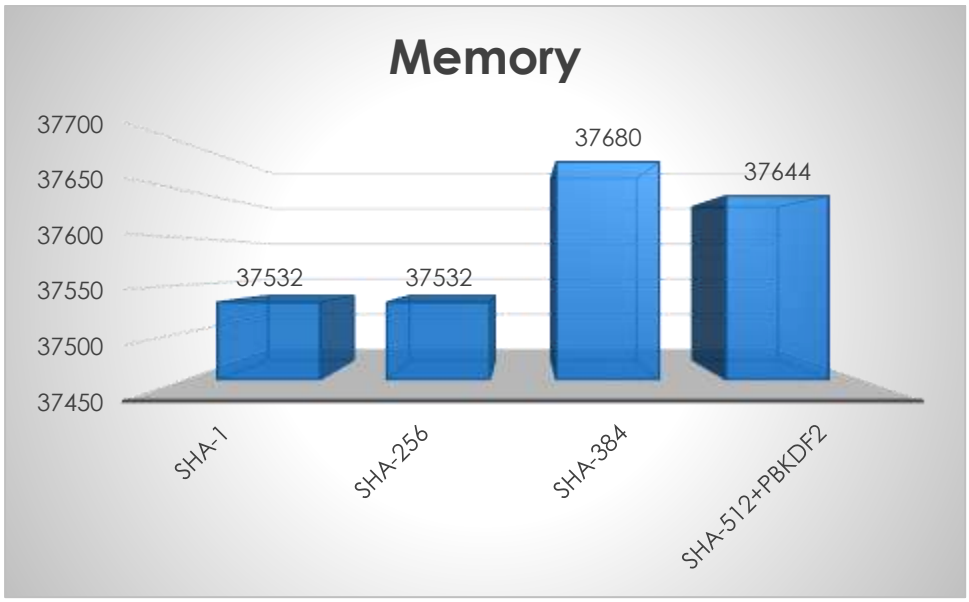

Figure 3: Comparison of Memory Occupied by Different SHA Algorithms Using Input 'abc'

Figure 4: Comparison of Execution Time in Milliseconds for Different SHA Algorithms Using Input 'abc'

The examination of cryptographic hash methods for the message/password "abc" reveals differences in processing speed but rather stable memory use. By CPU time, SHA-384 is the most efficient at 0.10 seconds, SHA-1 is second at 0.12 seconds, SHA-512+PBKDF2 is third at 0.13 seconds, and SHA-256 is last at 0.15 seconds, making it the slowest of the bunch. With SHA-1 and SHA-256 both using 37,532 units of memory, SHA-384 slightly higher at 37,680 units, and SHA-512+PBKDF2 at 37,644 units, there are hardly any changes in the amount of memory used.

The findings for CPU time are corroborated by the millisecond execution time: SHA-384 takes the cake at 1.429335 ms, SHA-256 comes in at 67.248105 ms, and SHA-1 and SHA-512+PBKDF2 both take around 76 ms. In terms of CPU and execution time, these results show that SHA-384 is the most efficient hash algorithm, and it does so without significantly increasing memory use. Faster execution does not always mean higher protection against assaults; hence, cryptographic resilience and security needs should also be considered when choosing an algorithm for real applications.

V. CONCLUSION

This study underscores the critical importance of safeguarding patient information in e-health cloud systems through advanced cryptographic techniques. By adopting a hybrid approach that integrates symmetric encryption for data security and asymmetric encryption for secure key exchange, supported by robust hashing algorithms, the proposed method effectively addresses the dual challenge of performance and security. The experimental analysis demonstrates that hybrid cryptography can deliver high levels of protection without imposing excessive computational

burdens, making it a practical choice for healthcare environments. The findings contribute valuable insights for healthcare providers, policymakers, and system developers in designing secure, efficient, and scalable e-health cloud solutions that uphold patient privacy and regulatory compliance.

REFERENCES

1. Dutta, R. Bose, S. Roy, and S. Sutradhar, "Hybrid Encryption Technique to Enhance Security of Health Data in Cloud Environment," Arch. Pharm. Pract., vol. 14, no. 3, pp. 41–47, 2023.
2. S. Gattoju and V. N. Lakshmi, "An Adaptive Wolf Based Dansing System for Securing Hadoop at the Data Cleaning Stage," SSRG Int. J. Eng. Trends Technol., vol. 70, no. 4, pp. 31–43, 2022.
3. P. R. Kumar et al., "Heart Disease Prediction based on Ensemble Classification Model with Tuned Training Weights," SSRG Int. J. Eng. Trends Technol., vol. 70, no. 4, pp. 59–81, 2022.
4. Boumezbeur and K. Zarour, "Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption," Acta Inf. Prag., vol. 11, no. 1, pp. 361–379, 2022.
5. Manuceau, "About a Fast Cryptographic Hash Function Using Cellular Automata Ruled by Far-Off Neighbours," SSRG Int. J. Eng. Trends Technol., vol. 69, no. 2, pp. 39–41, 2021.
6. Q. He and H. He, "A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining," Sustain., vol. 13, no. 1, pp. 1–17, 202.
7. Lee, "Comments on 'Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption'," IEEE Trans. Cloud Comput., vol. 8, no. 4, pp. 1299–1300, 2020.
8. Y. Liu, S. Xiao, H. Wang, and X. Wang, "New Provable Data Transfer from Provable Data Possession and Deletion for Secure Cloud Storage," Int. J. Distrib. Sens. Netw., vol. 15, no. 4, 2020.
9. S. Xiong, Q. Ni, L. Wang, and Q. Wang, "SEM-ACSIT: Secure and Efficient Multi Authority Access Control for IoT Cloud Storage," IEEE Internet Things J., vol. 7, no. 4, pp. 2914–2927, 2020.
10. Ogiela, M. R. Ogiela, and H. Ko, "Intelligent Data Management and Security in Cloud Computing," Sensors, vol. 20, no. 12, 2020.
11. Wu, C. Wang, and H. Yao, "Security Analysis and Secure Channel-Free Certificate Less Searchable Public Key Authenticated Encryption for a Cloud-Based Internet of Things," PLoS One, vol. 15, no. 4, pp. e0230722, 2020.
12. P. Singh and H. Pundir, "Secure File Storage on Cloud Using Cryptography," SSRG Int. J. Comput. Sci. Eng., vol. 7, no. 5, pp. 12–15, 2020.
13. N. Shaik, N. A. Ayedalshahrani, A. Saadalali, A. M. Alqahtani, and S. S. Hedan, "Making Digital Artifacts on the Web Verifiable and Reliable by using Cryptographic Hash Key," SSRG Int. J. Comput. Trends Technol., vol. 67, no. 11, pp. 38–41, 2019.