JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JETIR
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cryptography Techniques for Security in Cloud Data Storage

Shalu Saharawat
Lecturer Web Designing
Department of Computer Science and Engineering
Government Polytechnic, Kanpur, India

Abstract : Cloud and Internet of things application are growing day by day. Most of the organization are using the cloud storage services for own application. IOT application are building under the 5G wireless communication technologies. Security is the major concern for data security and safety. The basic techniques start from using the watermarking with advancement of the cryptography algorithm. Most of the online and cloud application are using the cryptography based data security. The most common and high secure cryptography algorithms are AES, RSA, and Hash etc. These paper presents cryptography techniques for security in cloud data storage.

***Index Terms* – Cryptography, Security, Cloud, Data, IOT.**

I. INTRODUCTION

Cloud figuring worldview is turning out to be extremely well known nowadays. In any case, it does exclude remote sensors and cell phones which are expected to empower new arising applications like distant home clinical checking. Subsequently, a consolidated Cloud-Web of Things (IoT) worldview gives adaptable on-request information stockpiling and versatile calculation power at the cloud side just as whenever, anyplace wellbeing information checking at the IoT side. Individuals store their information on cloud stockpiling usually now daily. Security is a significant issue in putting away information on clouds. Cryptography methods are extremely valuable to force security on information. In this paper a crossover cryptography framework is proposed to give better security on the information which is put away on cloud stockpiling [1].

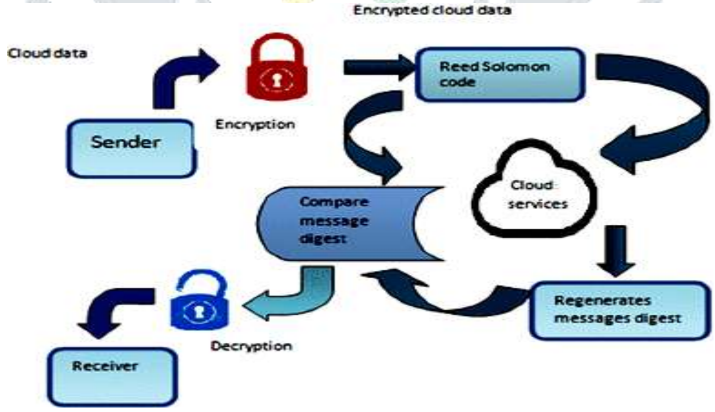


Figure 1: Cryptography Cloud Framework (google)

These days, Internet of Things (IoT) is an alluring framework to give wide network of a wide scope of uses, and clouds are regular advertisers. Cloud-helped IoT consolidates the upsides of cloud figuring and IoT, which can gather information from this present reality and augments the worth of the gathered information by the method for information sharing and information investigation. In the interim, secure and advantageous information recovery in cloud workers turns into a significant necessity for the two ventures and individual clients. Public key encryption with search usefulness (abbreviate as PKE-SF) is a generally utilized cryptographic procedure that permits clients to recover scrambled information without unscrambling. PKE-SF mostly contains the natives of public key encryption with watchword search (PKE-KS), public key encryption with fairness test (PKE-ET), and plaintext-checkable encryption (PCE) [2]. The cloud-helped clinical Web of Things (MIoT) plays had a progressive impact in advancing the nature of public clinical benefits. Nonetheless, the down to earth organization of cloud-helped MIoT in an open medical care situation raises the worry on information security and client's protection. Regardless of attempts by scholarly and mechanical local area to take out this worry by cryptographic strategies, asset obliged gadgets in MIoT might be dependent upon the substantial computational overheads of cryptographic calculations [3].

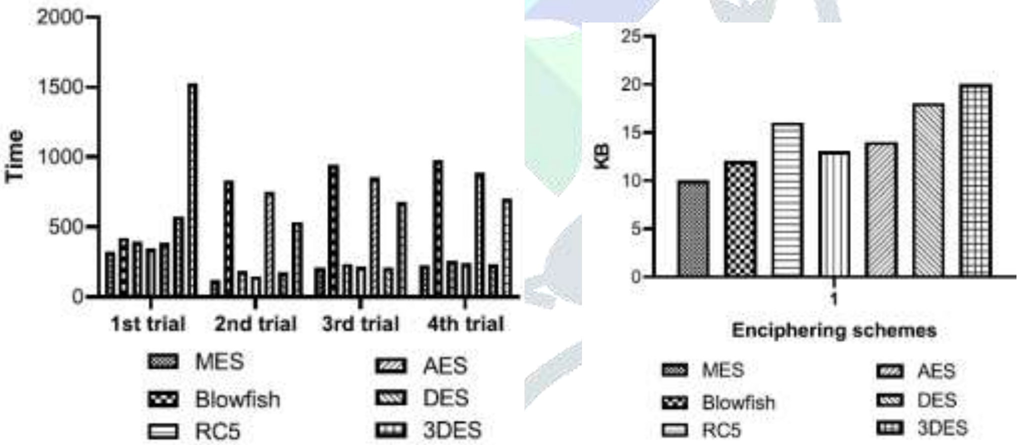
The development of web period prompts a significant change in a capacity of information and getting to the applications. One such recent fad that guarantees the perseverance is the Cloud figuring. Figuring assets presented by the Cloud incorporates the workers, organizations, stockpiling, and applications, all as administrations. With the appearance of Cloud, a solitary application is conveyed as a metered administration to various clients, by means of an Application Programming Interface (Programming interface) open over the organization. The administrations offered by means of the Cloud are like the foundation, programming, stage, data set and web administrations [4].

There is a worldwide promotion in the improvement of advanced medical services framework to cater the monstrous old populace and irresistible sicknesses. The computerized assistance is relied upon to guarantee the patient security, adaptability, and information trustworthiness on the touchy life basic medical care information, while adjusting to the worldwide medical services information assurance principles [5]. The patient information sharing to outsiders, for example, research organizations and colleges is additionally worried as a huge commitment to the general public to hone the exploration and examinations. The rise of 5G correspondence innovations kills the boundaries between patients, emergency clinic and different establishments with very good quality assistance guidelines. In patients' point of view, medical care administration conveyance through the advanced medium is gainful as far as time, expenses, and dangers [6]. The cloud-based Internet of-Things (IoT) has been applied to help pervasive information assortment and concentrated information preparing among different applications. Furnished with amazing assets, a semi-believed cloud can derive private data by dispatching derivation attack [7]. Homomorphic Encryption (HE) has been proposed as a successful method to save security from deduction attack while permitting certain calculation over ciphertext. In any case, HE prompts longer dormancy because of extra correspondence and calculation overheads [8]. Cloud framework abilities, including monstrous, versatile and flexible processing assets, have prompted the inescapable adaption of Web of Things (IoT) cloud-empowered administrations [9]. This includes moving the capacity and handling of touchy IoT information to Cloud Specialist organizations (CSPs) that gain total admittance to rethought IoT information in the cloud. An effective and lightweight Progressed Encryption Standard cryptosystem can assume a significant part in shielding IoT information from being presented to CSPs by securing the protection of touchy rethought information [10].

II. LITERATURE SURVEY

W. Almuseelem et al.,[1] presented a new security, load balancing, and energy-aware task offloading framework for the ECC system environment to bypass potential security threats and the edge servers' balancing challenge. Specifically, a new layer of security based on an advanced encryption standard (AES) cryptographic method and fingerprint combination is introduced in order to protect the data from vulnerabilities during offloading.

M. Shabbir et al.,[2] presented the Modular Encryption Standard (MES) based on the layered modeling of the security measures. The performance analysis shows that the proposed work excels, compared to other commonly used algorithms against the health information security at the MCC environment in terms of better performance and auxiliary qualitative security ensuring measures.



(a) (b)

Figure 2: (a) Processor utilization rate (b) Memory utilization [2]

A. Kumar et al.,[3] presents the methodology which use RSA calculation and DES calculation and give a half breed of the two calculations to give greater security on the information prior to putting away it on cloud. The proposed calculation is carried out in JAVA and test on an example plain text. The paper will be exceptionally helpful for IOT applications putting away information on cloud. It is checked that the proposed calculation is functioning admirably to give greater security on information.

H. Xiong et al.,[4] presented these plans according to alternate points of view to give better understanding to amateurs and progressed scientists. All the more solidly, this review focuses on the cutting edge of PKE-SF by breaking down the plan reasoning, looking at the system and security model, and surveying the current plans as per hypothetical proficiency, security properties and trial execution. Besides, we talk about the augmentations of customary PKE-SF plans which include with the entrance control appointment, conjunctive watchword search, declaration free and disconnected catchphrase speculating attack flexibility.

Y. Bao et al.,[5] presented a productive, revocable, security safeguarding fine-grained information imparting to catchphrase search (ERPF-DS-KS) conspire, which understands the proficient and fine-grained admittance control and ciphertext watchword search, and empowers the adaptable circuitous denial to pernicious information clients. A pseudo personality based mark system is intended to give the information credibility. We dissect the security properties of our proposed conspire, and by means of the hypothetical correlation and exploratory outcomes we show that for the asset obliged gadgets in the patient and specialist side of MIoT, in examination with other related plans, ERPF-DS-KS simply devours the lightweight and steady size correspondence/stockpiling just as computational time cost.

D. Samanta et al.,[6] presented, SVM based encryption administration model is built for which the key age is from the customary encryption activity mode for certain enhancements. To make the cycle more perplexing, the improvement strategies are considered for the vital age in relative two techniques application model that acts computationally safer explicitly for Cloud climate. The consequences of safety examination affirm the adequacy of the proposed application model withstands conceivably against different attacks, for example, Picked Code Attack, Picked Plain text Attack undefined attacks for documents. If there should be an occurrence of pictures, it opposes well against factual and differential attacks. Similar Investigation shows proof of the productivity of the created spearheading application model quality and strength contrasted and that of the current administrations.

G. Kuldeep et al.,[7] presented a plan of the multi-class security protecting cloud processing plan (MPCC) utilizing compressive detecting for reduced sensor information portrayal and mystery for information encryption. The proposed conspire accomplishes two-class mystery, one for superuser who can recover the specific sensor information, and the other for semi-approved client who is simply ready to acquire the measurable information like mean, change, and so forth MPCC plot permits computationally costly scanty sign recuperation to be performed at cloud without compromising the classification of information to the cloud specialist organizations.

T. Hewa et al.,[8] presented a clever Multi-access Edge Computing(MEC) and blockchain based assistance design using the lightweight ECQV (Elliptic Bend Qu-Vanstone) declarations for the realtime information security, respectability, and validation between IoT, MEC, and cloud. The entrance control is dealt with through the shrewd agreements. We assessed the proposed framework in a close to reasonable execution utilizing Hyperledger Texture blockchain stage with Raspberry Pi gadgets to recreate the movement of the clinical sensors.

Table 1: Cryptography techniques comparison

Algorithms	Blow Fish	AES	3DES	DES
Key size (bits)	32-448	128,192,256	112 or 118	64
Block size (bits)	64	128	64	64
Round	16	10,12,14	84	16
Structure	Feistel	Substitution Permutation	Feistel	Feistel
Flexible	Yes	Yes	Yes	No
Features	Secure enough	Excellent Security	Adequate security replacement for DES	Not enough structure
Speed	Fast	Fast	Very Slow	Slow

Y. Jiang et al.,[9] presented an enhancement structure in protection saving access control under cloud-mist registering frameworks. The enhancement objective is to boost the normal client fulfillment in the framework, where cost and idleness fill in as key measurements estimating client fulfillment. Because of the NP-hardness of the defined issue, we propose a low-intricacy problematic calculation to address it, where the entrance offloading dynamic, client collaboration, and asset allotment are thought of. Recreation results are introduced to show the benefits of our proposed calculation as far as the normal USI (Client Fulfillment File) and the quantity of clients with zero USI.

A. Alabdulatif et al.,[10] presented, AES cryptosystems need calculation abilities, which is a basic factor that forestalls us exploiting cloud figuring administrations. When utilized with AES cryptosystems, Intel Programming Gatekeeper Expansions (SGX) can give an exhaustive answer for building secure information examination system for IoT-empowered application in different areas. In this paper, we foster a safe information investigation system that depends on a hyper-incorporated methodology where both programming and equipment based arrangements are applied to secure and handle touchy re-appropriated information in the cloud.

K. Albalawi et al.,[11] presented the plan to take the upsides of BC innovation in further developing the IoT network security. Specifically, we propose a security structure for IoT organizations to improve the gadgets' validation. The proposed design comprises of three layers, blockchain layer, authenticator layer and requester layer. The gadgets' confirmation cycle is isolated into two stages: gadget enlistment stage, and gadget validation stage. The proposed structure fulfills the three mainstays of safety to be specific, privacy, trustworthiness, and accessibility. Classification is accomplished by restricting the admittance to approved gadget just which keep the information stowed away from untouchables. Trustworthiness is ensured by utilizing BC that keeps up with the information from being modified. Accessibility is guaranteed by keeping up with the BC information base on the cloud.

H. A. Al Hamid et al.,[12] presented the main focus has been given to secure healthcare private data in the cloud using a fog computing facility. To this end, a tri-party one-round authenticated key agreement protocol has been proposed based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely. Finally, the private healthcare data are accessed and stored securely by implementing a decoy technique.

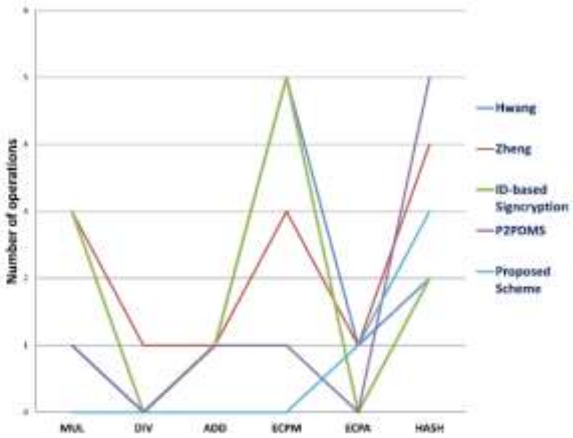


Figure 3: Comparison graph between the existing scheme [12]

Table 2: RSA and ECC performance, security, and space requirements comparison [12]

	Key Generation Time	Memory requirement	Encrypt /Decrypt Time
ECC (106 bits)	57 ms	108 bytes	11 ms
RSA (512 bits)	383 ms	157 bytes	77 ms
ECC (132 bits)	98 ms	117 bytes	17 ms
RSA (768 bits)	889 ms	236 bytes	160 ms
ECC (160 bits)	108 ms	125 bytes	16 ms
RSA (1024 bits)	2609 ms	313 bytes	338 ms
ECC (210 bits)	121 ms	140 bytes	15 ms
RSA (2048 bits)	18399 ms	621 bytes	1867 ms

III. CHALLENGES AND SOLUTIONS

Here are some of the key challenges in detail:

1. **Data Privacy and Compliance:**

   - Challenge: Different countries have various data protection laws and regulations (e.g., GDPR, HIPAA, CCPA). Complying with these regulations while using cloud storage can be complex.

   - Solution: Understand the legal requirements in your jurisdiction and choose a cloud provider that offers tools and features to assist in compliance.

2. **Data Leakage and Unauthorized Access:**

   - Challenge: Ensuring data isn't accessed or leaked without proper authorization is crucial but can be challenging with numerous potential access points.

   - Solution: Implement robust access control mechanisms, employ encryption, and monitor data access for unusual behavior.

3. **Shared Responsibility Model:**

   - Challenge: Understanding the division of security responsibilities between the cloud provider and the user is crucial but can lead to misunderstandings.

- Solution: Clearly define and document responsibilities. The cloud provider typically secures the infrastructure, while users are responsible for securing their data and access.

4. **Data Loss:**

- Challenge: Data stored in the cloud can be vulnerable to loss due to hardware failures, natural disasters, or other unforeseen events.

- Solution: Regularly back up data and choose cloud providers with robust redundancy and disaster recovery capabilities.

5. **Data Encryption Management:**

- Challenge: Managing encryption keys securely and ensuring proper key rotation can be complex and error-prone.

- Solution: Use dedicated key management systems, Hardware Security Modules (HSMs), or key management services provided by the cloud provider.

6. **Security Breaches:**

- Challenge: Security breaches or vulnerabilities in cloud infrastructure can expose your data to unauthorized parties.

- Solution: Stay updated on security best practices, promptly patch vulnerabilities, and employ intrusion detection systems and incident response plans.

7. **Data Portability:**

- Challenge: Moving data between different cloud providers can be challenging, leading to vendor lock-in.

- Solution: Use open standards and consider multi-cloud or hybrid cloud strategies to maintain data portability.

8. **Network Security:**

- Challenge: Data is transferred over public networks, making it susceptible to eavesdropping.

- Solution: Use encryption (e.g., SSL/TLS) for data in transit and implement secure network configurations.

IV. CONCLUSION

This paper presents cryptography techniques for security in cloud data storage. Various researches proposal and outcomes are included in the paper. The cloud-IOT based security challenges, encryption mistakes are considered. Some of the best cryptography approaches like DES, AES, RSA, Hash, and Blowfish etc are studied in the existing research work. In the future make hybrid algorithm based on the cryptography and apply in the cloud based IOT applications.

REFERENCES

1. W. Almuseelem, "Energy-Efficient and Security-Aware Task Offloading for Multi-Tier Edge-Cloud Computing Systems," in IEEE Access, vol. 11, pp. 66428-66439, 2023, doi: 10.1109/ACCESS.2023.3290139.
2. M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.
3. A. Kumar, V. Jain and A. Yadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), 2020, pp. 514-517, doi: 10.1109/PARC49193.2020.236666.
4. H. Xiong, T. Yao, H. Wang, J. Feng and S. Yu, "A Survey of Public Key Encryption with Search Functionality for Cloud-assisted IoT," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3109440.
5. Y. Bao, W. Qiu, P. Tang and X. Cheng, "Efficient, Revocable and Privacy-preserving Fine-grained Data Sharing with Keyword Search for the Cloud-assisted Medical IoT System," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2021.3100871.
6. D. Samanta et al., "Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture," in IEEE Access, vol. 9, pp. 98013-98025, 2021, doi: 10.1109/ACCESS.2021.3095297.
7. G. Kuldeep and Q. Zhang, "Compressive Sensing based Multi-class Privacy-preserving Cloud Computing," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348093.
8. T. Hewa, A. Braeken, M. Ylianttila and M. Liyanage, "Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348125.

9. Y. Jiang, K. Zhang, Y. Qian and L. Zhou, "An Optimization Framework for Privacy-preserving Access Control in Cloud-Fog Computing Systems," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348516.
10. A. Alabdulatif, "Secure Data Analytics for IoT Cloud-enabled Framework Using Intel SGX," 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2020, pp. 54-57, doi: 10.1109/WETICE49692.2020.00019.
11. K. Albalawi and M. M. A. Azim, "Cloud-based IoT Device Authentication Scheme using Blockchain," 2019 IEEE Global Conference on Internet of Things (GCIoT), 2019, pp. 1-7, doi: 10.1109/GCIoT47977.2019.9058391.
12. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in IEEE Access, vol. 5, pp. 22313-22328, 2017, doi: 10.1109/ACCESS.2017.2757844.