

Security Techniques in Cloud Computing for Cloud Data Storage

Akshay Bedse¹, Puja Padiya² and Amarsinh Vidhate³

¹⁻³Ramrao Adik Institute of Technology, Nerul Navi Mumbai, India
Email: akshaybedse@gmail.com, {padiya.puja, amar.vidhate}@rait.ac.in

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, Hash etc. This paper presents the cryptography techniques and challenges for the security in cloud data storage for IOT applications.

Index Terms— cloud computing, cloud, cryptography, data, iot, security.

I. INTRODUCTION

Cloud registering worldview is turning out to be extremely famous nowadays. Be that as it may, it does exclude remote sensors and cell phones which are expected to empower new arising applications like remote home clinical observing. In this manner, a consolidated Cloud-Web of Things (IoT) worldview gives versatile on-request information capacity and strong calculation power at the cloud side as well as whenever, anyplace wellbeing information checking at the IoT side. Individuals store their information on cloud capacity generally now daily. Security is a significant issue in putting away information on clouds. Cryptography strategies are exceptionally valuable to force security on information. In this work a crossover cryptography framework is proposed to give better security on the information which is put away on cloud capacity [1]. These days, Web of Things (IoT) is an alluring framework to give wide availability of a wide scope of utilizations, and clouds are regular advertisers. Cloud-helped IoT joins the upsides of cloud registering and IoT, which can gather information from this present reality and boosts the worth of the gathered information by the method for information sharing and information investigation. In the mean time, secure and advantageous information recovery in cloud servers turns into a significant prerequisite for the two undertakings and individual clients. Public key encryption with search usefulness (abbreviate as PKE-SF) is a broadly utilized cryptographic strategy that permits clients to recover scrambled information without decoding. PKE-SF mostly contains the natives of public key encryption with watchword search (PKE-KS), public key encryption with equity test (PKE-ET), and plaintext-checkable encryption (PCE) [2]. The cloud-helped clinical Web of Things (MIoT) plays had a progressive influence in advancing the nature of public clinical benefits. Be that as it may, the pragmatic sending of cloud-helped MIoT in an open medical services situation raises the worry on information security and client's protection. In spite of attempts by scholarly and modern local area to dispense with this worry by cryptographic techniques, asset compelled gadgets in MIoT might be dependent upon the weighty computational overheads of

cryptographic calculations [3].

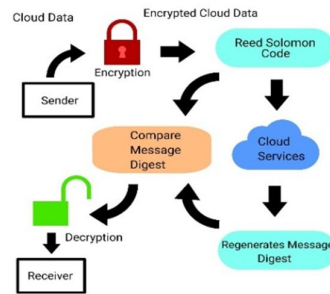


Figure 1: Cryptography cloud system

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 servers, organizations, stockpiling, and applications, all as administrations. With the approach of Cloud, a solitary application is conveyed as a metered administration to various clients, through an Application Programming Point of interaction (Programming interface) available over the organization. The administrations offered through the Cloud are, for example, the foundation, programming, stage, information base and web administrations [4].

There is a worldwide publicity in the improvement of computerized medical services framework to cook the monstrous older populace and irresistible infections. The advanced help is relied upon to guarantee the patient security, adaptability, and information uprightness on the delicate life basic medical care information, while adjusting to the worldwide medical care information insurance guidelines. 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 development of 5G correspondence advancements annihilates the boundaries between patients, clinic and different foundations with very good quality help principles. In patients' viewpoint, medical care administration conveyance through the advanced medium is gainful as far as time, expenses, and dangers [6]. The cloud-based Web of-Things (IoT) has been applied to help universal information assortment and unified information handling among different applications. Outfitted with strong assets, a semi-believed cloud can reason private data by sending off derivation assault. Homomorphic Encryption (HE) has been proposed as a successful method for protecting security from deduction assault while permitting specific calculation over ciphertext. Be that as it may, HE prompts longer inertness because of extra correspondence and calculation overheads [7]. Cloud foundation abilities, including huge, versatile and flexible figuring assets, have prompted the far and wide adaption of Web of Things (IoT) cloud-empowered administrations. This includes moving the capacity and handling of delicate IoT information to Cloud Specialist co-ops (CSPs) that gain total admittance to reevaluated IoT information in the cloud. A productive and lightweight Advance Encryption Standard (AES) cryptosystem can assume a significant part in safeguarding IoT information from being presented to CSPs by safeguarding the security of delicate re-appropriated information [8].

II. LITERATURE SURVEY

A. Kumar et al.,[1] presents the methodology which use RSA calculation and DES calculation and give a cross breed of the two calculations to give greater security on the information prior to putting away it on cloud. Besides, we talk about the augmentations of conventional PKE-SF plans which include with the entrance control assignment, conjunctive watchword search, declaration free and disconnected catchphrase speculating assault versatility.

H. Xiong et al.,[2] presents these plans according to alternate points of view to give better appreciation to fledglings and progressed specialists. All the more solidly, this overview focuses on the best in class of PKE-SF by investigating the plan reasoning, looking at the system and security model, and surveying the current plans as per hypothetical productivity, security properties and trial execution.

Y. Bao et al.,[3] proposes a proficient, revocable, security saving fine-grained information offering to catchphrase search (ERPF-DS-KS) conspire, which understands the productive and fine-grained admittance control and ciphertext watchword search, and empowers the adaptable backhanded disavowal to pernicious

information clients. A pseudo personality-based signature component is intended to give the information realness.

D. Samanta et al.,[4] make the interaction more mind boggling, the improvement procedures are considered for the critical age in relative two techniques application model that acts computationally safer explicitly for Cloud climate. The aftereffects of safety investigation affirm the viability of the proposed application model endures conceivably against different assaults, for example, Picked Code Assault, Picked Plain text Assault unclear assaults for documents. In the event of pictures, it opposes well against factual and differential assaults.

G. Kuldeep et al.,[5] presents plan of the multi-class security protecting cloud processing plan (MPCC) utilizing compressive detecting for smaller sensor information portrayal and mystery for information encryption. This work, proposed a calculation in light of Actual layer key age (PLKG) and Actual layer encryption (PLE) as a safeguarding measure. Additionally, this work examines the high-level encryption standard (AES) and make a similar report to demonstrate it's greatly gotten, viable and quick encryption highlights among the other accessible strategies and presumes that AES produces a superior arrangement.

T. Hewa et al.,[6] propose a clever Multi-access Edge Computing (MEC) and blockchain based assistance design using the lightweight ECQV (Elliptic Bend Qu-Vanstone) endorsements for the realtime information security, uprightness, and confirmation between IoT, MEC, and cloud. We further joined stockpiling offloading capacity to the blockchain to guarantee versatility with a monstrous number of associated clinical gadgets to the cloud. We acquainted a compensating plan with the patients and medical clinics through the blockchain to energize information sharing.

Y. Jiang et al.,[7] propose a streamlining structure in security saving access control under cloud-mist registering frameworks. The streamlining objective is to augment the normal client fulfillment in the framework, where cost and dormancy fill in as key measurements estimating client fulfillment. Because of the NP-hardness of the planned issue, we propose a low-intricacy sub-par calculation to tackle it, where the entrance offloading independent direction, client collaboration, and asset distribution are thought of. Reproduction results are introduced to show the benefits of our proposed calculation as far as the normal USI (Client Fulfillment List) and the quantity of clients with zero USI.

A. Alabdulatif et al.,[8] Notwithstanding, AES cryptosystems need calculation capacities, which is a basic component that forestalls us exploiting cloud figuring administrations. The data that we keep in clouds is probably going to be manhandled by an unapproved individual or the cloud experts to collaborate itself. The work gives a concise thought of cloud registering information security, and different strategies are utilized in guaranteeing the security of information and we have looked at different encryption calculation utilized for encoding information in the cloud.

K. Albalawi et al.,[9] give the intend to take the upsides of BC innovation in further developing the IoT network security. Specifically, we propose a security system for IoT organizations to upgrade the gadgets' verification. The proposed engineering comprises of three layers, blockchain layer, authenticator layer and requester layer. The gadgets' confirmation interaction is separated into two stages: gadget enlistment stage, and gadget verification stage. The proposed system fulfills the three mainstays of safety specifically, secrecy, honesty, and accessibility. Privacy is accomplished by restricting the admittance to approved gadget just which keep the information stowed away from untouchables. Uprightness is ensured by utilizing BC that keeps up with the information from being changed. Accessibility is guaranteed by keeping up with the BC data set on the cloud.

M. A. Kiran et al.,[10] proposed conspire accomplishes security prerequisites, for example, shared verification, the security of a mystery key, meeting key arrangement, opposes imitation assault, opposes an insider assault, opposes replay assault and opposes pantomime assault. The security investigation demonstrates that our plan is secure against different known assaults. Execution investigation shows that our plan is lightweight and appropriate for the asset imperative IoT gadgets.

Q. W. Ahmed et al.,[11] Today cloud figuring is arising as an imperative variable in our everyday lives. Its acclaim is increasing at a remarkable rate alongside its development. It serves its client with unmistakable figuring abilities like calculation, stockpiling, organizing, applications, and so on, over the web upon a specific solicitation. Among all the above abilities, capacity assumes a pivotal part in working with its client by giving its system on lease premise. Despite the fact that cloud registering is having a ton of advantages, its acknowledgment is as yet falling behind because of safety concerns.

A. Dey et al.,[12] The interest of higher range transmission capacity can nearly have relieved now-a-days by the utilization of Web of Things (IoT) based 5G correspondence organizations. IoT is certainly standing out a result of the intricacy elements of IoT gadgets. Its less power imperatives property have diminished the use of customary cryptographic strategies however it has utilized the Confided in stage module (TPM) for validation and Believed network associate (TNC) norms to screen the vindictive programming or firmware.

A. Kamble et al.,[13] proposes a thought of Wellbeing Observing Framework which screens the physiological boundaries of the patient which incorporates Temperature, heartbeat, ECG, with the utilization of these sensors which can be associated with Raspberry Pi Board that communicates the information to a nearby server. In the event of any odd conduct or any basic signs and manifestations are perceived, the overseer notwithstanding clinical specialists are advised by right way through the message or Email.

A. Kumari et al.,[14] presents an effective Remote Checking Framework, Security is of central significance. in this way to give security to the patient's information Shamir's Mystery key Sharing Calculation is utilized in which information and keys will get parted, saved at various area and to recover them limit cryptography is utilized. For Coronary illness finding the expectation calculation support vector machine (SVM) is utilized. Accordingly, the framework presents quality medical services to all.

C. Thirumalai et al.,[15] presents a plan reuses the RSA plot with a Diophantine type of the nonlinear condition. Also, our plan execution relatively performs well and this mostly because of the utilization of RSA public key alone. Because of this, our MEMK doesn't need multiplicative opposite work or Broadened Euclid's calculation. At last, we have made a test result on different periods of MEMK PKC like key age, encryption, and decoding by changing the N-bit modulo bits from 1K to 10K.

III. CHALLENGES

What are the difficulties cloud shoppers and cloud specialist organization's face with regards to information encryption? These are as per the following:

A. Cloud platform differences

Contrasts in cloud stages present inconveniences in information encryption. There are three models with respect to the cloud stage and these are Foundation as an Assistance (IaaS), Stage as a Help (PaaS), and Programming as an Assistance (SaaS). Every one of these models offers security arrangements and perform various assignments to give security to a tremendous measure of information. In view of the distinctions between these models present, there are intricacies in the encryption draws near. As an outcome, an association's cloud specialist co-op will find it difficult to keep up with and perform different encryption processes.

B. Key management complexity

Managing information encryption, key administration is the most muddled issue of any security framework and organization. Key administration is the most common way of shielding encryption keys from misfortune, unapproved access, and debasement. Notwithstanding, key administration is generally the significant explanation encryption isn't being executed by associations. As indicated by John Droge of Raytheon, a network protection arrangements organization, "key administration is the most troublesome discipline inside cryptography and requires outrageous scrupulousness by each merchant and client/administrator in the data."

C. Diversity of encryption architectural approaches

There are a great deal of design approaches for encryption in the cloud, for example, application level, document framework based, specialist based, and capacity gadget level methodology, as per the Cloud Norms Client Gathering. These methodologies have their own highlights in view of the administration of encryption keys and their exhibitions. During the cycle, additionally, different calculations are distinctively used. Thus, it is hard and testing to lay out associations and correspondence among these methodologies.

D. Assess your cloud security

Consistence guidelines in various areas or nations One of the cloud issues in involving information encryption is the assortment of consistence guidelines in various regions. In this way, information encryption isn't direct and goes through different cycles before it finishes. For example, in the event that a business is expected to agree with a guideline in its nation, yet its information is globally put away and encoded, other consistence guidelines in different nations could perform information appraisal first. In outcome, the cloud stockpiling supplier will bound to find it difficult to oversee and perform encryption on this event.

E. The challenge of responsibility

As indicated by a review directed by Thales e-Security and Ponemon Establishment, the most liable for safeguarding cloud information are cloud specialist organizations, trailed by cloud customers. As a result of the difficulties referenced above, whoever assumes the liability of information encryption should survive and

oversee them all. Cases of this challenge could be an upsurge in monetary costs and convoluted correspondence and cooperation between both the cloud specialist co-op and the cloud shopper.

F. Security Issues to Consider When Encrypting Cloud Data

While encryption in the cloud appears to be the silver slug in information security, it shouldn't be seen along these lines, as shown by Gartner, a main exploration and warning organization. As indicated by Gartner, associations ought to set up an information security plan first with regards to cloud encryption. In the event that ventures neglect to do as such, it could bring about more intricacies and monetary issues. There are some cloud stockpiling security issues and dangers to contemplate on when associations store and encode their information in the cloud.

The greatest issue is the secret phrase or the security key. In the event that the appointed secret key is lost during the course of encryption in the cloud, it's basically impossible to rescue the information. One more issue about passwords is that individuals make normal words, like their email passwords or mate's name. The simpler the security key to figure, the more straightforward the information can be penetrated.

Also, one of the cloud issues with encryption is the misguided feeling that all is well and good. Encryption guarantees that encoded information can't be attacked and taken in view of its complicated cycles and methods. In any case, there is no ideal answer for information security. The association sees encryption to have numerous assets expected that is the reason it's considered to be the best arrangement. Its intricacy makes this misguided feeling that all is well and good. It's anything but a fix all arrangement.

One more security issue to think about while scrambling cloud information is that it requires participation. For example, assuming an individual from an association shares a document that needs mystery to another part, this record ought to be constantly encoded while sending. Nonetheless, both of the individuals could figure out it opportunity consuming and exhausting to encode and decipher that information. Encryption requires participation and this can be trying to all gatherings included.

IV. COMMON CLOUD ENCRYPTION MISTAKES

Associations and security experts see cloud encryption solid and completely secure. However, the right inquiry to pose is this: why are endeavors and, surprisingly, the public authorities actually get hacked and break? The response is they're not doing it right.

Here are a portion of the missteps associations make while scrambling cloud information:

A. Reliance on low-level encryption

Low-level encryption is considered to be a single tick answer for information break counteraction. Instances of this are circle and record encryption. This is generally performed by fledglings. Be that as it may, it is perilous to fundamentally rely upon this sort of arrangement. For example, while the server is off, plate encryption just works during that time. The working framework will unscramble information when the server is turned on and the information will be open to all clients that are signed in. Dependence on low-level encryption is just about as simple as a single tick, however assailants will be calm at penetrating.

B. Assuming that software developers have full expertise

Programming designers and specialists are regularly not specialists in security. Specialists are as a rule in the IT field and they are pen analyzers, CISOs, and framework heads. Associations depend on programming designers since they're great at taking care of troublesome issues. In any case, with regards to information encryption, they can fall flat at execution. A portion of the missteps of programming engineers incorporate unprotected encryption keys, unprotected keystore, powerless crypto, utilizing old libraries, and involving one key for everything.

C. Dependence on cloud providers when it comes to data security

Since information breaks have been expanding over the long haul, increasingly more innovation organizations give cloud capacity administrations. Tech monsters like Google, Microsoft, and Amazon burn through large number of dollars to be the most reliable cloud in the network protection industry. Along these lines, associations expect to be that assuming they profit of these organizations' cloud benefits, their information will have full security under these suppliers. That is a hazardous supposition. In opposition to the review by Thales e-Security and Ponemon Organization referenced above, practically all cloud suppliers express that cloud customers have the most obligation in getting information. Indeed, even Amazon Web Administrations made a diagram representing the obligation of the shoppers and this incorporates information encryption.

D. Incorrect key management

Getting key administration wrong is the greatest mix-up an association can make. Regardless of whether the information is encoded the correct way, inappropriate treatment of key administration could prompt information breaks. This is much the same as spending on the best lock on the planet and putting away it under the mat. Key administration disappointments incorporate bringing the key shakily, leaving the key unprotected with one more layer of the encryption key, utilizing a similar key and never evolving it.

V. CONCLUSION

This paper presents the cryptography methods for security in cloud information capacity for IOT applications. Different investigates proposition and results are remembered for the work. The cloud-IOT based security challenges, encryption botches are thought of. The absolute best cryptography approaches like DES, AES, RSA, Hash, and Blowfish and so on are examined in the current examination work. Later on make half breed calculation in view of the cryptography and apply in the cloud based IOT applications.

REFERENCES

- [1] 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/PARC49193.2020.2366666.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] M. A. Kiran, S. Kumar Pasupuleti and R. Eswari, "A Lightweight Two-factor Mutual Authentication Scheme for Cloud-based IoT," 2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2019, pp. 1-6, doi: 10.1109/ICRAIE47735.2019.9037779.
- [11] Q. W. Ahmed and S. Garg, "A Cloud computing-based Advanced Encryption Standard," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 205-210, doi: 10.1109/I-SMAC47947.2019.9032581.
- [12] A. Dey, S. Nandi and M. Sarkar, "Security Measures in IOT based 5G Networks," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 561-566, doi: 10.1109/ICICT43934.2018.9034365.
- [13] A. Kamble and S. Bhutad, "IOT based Patient Health Monitoring System with Nested Cloud Security," 2018 4th International Conference on Computing Communication and Automation (ICCCA), 2018, pp. 1-5, doi: 10.1109/CCAA.2018.8777691.
- [14] A. Kumari, V. Kumar, M. YahyaAbbasi and M. Alam, "The Cryptanalysis of a Secure Authentication Scheme Based on Elliptic Curve Cryptography for IOT and Cloud Servers," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2018, pp. 321-325, doi: 10.1109/ICACCCN.2018.8748591.
- [15] C. Thirumalai and H. Kar, "Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1-6, doi: 10.1109/IPACT.2017.8244948.