SECURITY OF CLOUD APPLICATIONS WITH HYBRID ENCRYPTION

Suresh Kumar B

Lecturer in Electronics Engineering, Government Polytechnic College, Palakkad, Kerala

ABSTRACT

Sensitive data on the cloud has grown exponentially, increasing its vulnerability. Unquestionably, the vulnerability stems from the growing number of users with malevolent intent. Given that cloud data and services are housed in data centres and that the cloud is managed by a third party, it is imperative to provide cloud security services. Data can be encrypted by anybody using the public key; however, data can only be decrypted by those who possess the private key. When using hybrid encryption, each message's plaintext is encrypted to create a cipher text by the sender creating a new symmetric key. The public key of the recipient is wrapped in that symmetric key. Presently, every feasible application of public key cryptography makes use of a hybrid system. Because more people are using the cloud for a variety of reasons, there is a greater need for extremely safe and secure data. In light of the aforementioned considerations and in order to establish a secure atmosphere, this work suggests a hybrid encryption algorithm that combines symmetric and asymmetric cryptography techniques in a way that is appropriate for modern cloud security and privacy protection. In order to achieve data confidentiality and cloud security, we propose a privacy model that uses Advanced Encryption Standard (AES) as the first level data encryption scheme prior to cloud application data storage. Elliptic Curve Cryptography (ECC) is the subsequent encryption scheme with AES key. Examples include the TLS protocol and the SSH protocol, that use a public-key mechanism for key exchange (such as Diffie-Hellman) and a symmetric-key mechanism for data encapsulation (such as AES).

Keywords: *Hybrid Encryption; Advanced Encryption Standard; Elliptic Curve Cryptography*

INTRODUCTION

The term "cloud" describes the collective strength of the Internet's accessible processing capacity. The National Institute of Standard and Technology (NIST) defines cloud computing (CC) as a standard environment that is typified by appropriate, widespread, on-demand network access to shared, robust, configurable computing resources that are available for lease at a very reduced management as well as little interference from the providers. As cloud-based apps grow in popularity, cloud application security is becoming an increasingly important concern. A modular approach to application development is made possible by the cloud, allowing development and operations teams to produce feature-rich apps more quickly. Nonetheless, the very qualities that make cloud-local applications deft and nimble can likewise present an assortment of cloud application security chances. Consolidating cloud application security rehearsals is a successful way for associations to keep away from application security gambles, guarantee an easily running programming improvement lifecycle (SDLC), and lay out an overall solid security posture. Nonetheless, executing these practices inside DevSecOps groups can frequently be very difficult for complex, micro service-based, cloud-local applications. Some of the required assets are networks, servers, capacity, applications, and administrations. The adaptable notwithstanding unique structure of CC gives a versatile data innovation limit in administrations as conveyed over the Web clients. [1] There has been a quick improvement in advancements, which has expanded the quantity of specialist organizations and clients taking on cloud computing. Distributed computing, in Buyya et al. [2], was alluded to as 'the fifth utility', notwithstanding water, power, phone, and gas as the promptly accessible on-request registering administrations over the web in the present human culture. It has been for the most part acknowledged and utilised in administration, online business stages, and the military to guarantee networks with solid accessibility. This shows up with the Cloud Specialist organisation (CSP) giving and keeping up with the expected information base and its application from a distance; it permits free pervasive access through an organisation. Cloud administration classes are arising; the main three are: programming as an administration (SaaS), stage as a help (PaaS), and foundation as an administration (IaaS). Albeit, CC takes various benefits over the customary information stockpiling; information security has been the shoppers' scourge to embracing its full administrations, inferable from the way that most cloud administrations are overseen by an outsider. This has raised a few concerns about information stockpiling since clients' impact on the specific information area or different types of information put away along with their information is obscure. In any case, in spite of clients' unsettlingness, since CC development, laid-out firms, for example, IBM, Google, Yippee, eBay, and Amazon, have put and proceeded to put altogether into CC and its foundation; huge quantities of clients, including states of different countries, share enormous amounts of information from various areas across the globe with high velocity to upgrade their particular administrations to clients and residents at large. Consequently, guaranteeing information security, protection, honesty, and accessibility to cloud clients with presently sent approaches appears to be lacking to achieve end clients' information security. An encryption plan will be expected to ensure protection and conservation of clients' information in a determined state. To guarantee cloud information security, a cross-breed encryption calculation, which includes utilising two crypto-plans: a symmetric High Level Encryption Standard (AES) and a hilter-kilter calculation called Elliptic Bend Cryptography (ECC), Utilizing a symmetric calculation also called private key cryptography with a solitary key for encryption and unscrambling combined with an uneven calculation (that is, public-key cryptography (PKC)) to upgrade the cloud information security as expected for the prescribed procedures. The symmetric key encryption is of extraordinary benefits in term of speed, and calculation time anyway open key encryption has preferable key administration over confidential key encryption. Public-key cryptography was designed to proffer answer for the symmetric-key cryptography challenges [3]. The proposed approach gives a half and half encryption plot utilizing AES and ECC to improve the cloud information security by scrambling information utilizing AES then encode AES key with ECC when in cloud. This paper examines different cryptographic encryption techniques and furthermore gives a half and half encryption strategy to a cloud application. As of late, numerous associations embraced a light-footed programming improvement process known as DevOps. This approach consolidates conventional programming advancement and IT activities to speed up the improvement life cycle and quickly discharge new programming applications. Nonetheless, conventional organization, application and framework safety efforts commonly don't safeguard cloud-based applications, hence making them defenseless against a large group of cyberattacks during improvement. Associations that are utilizing the cloud, especially as a feature of the product improvement process, should now plan and execute an exhaustive cloud security answer for safeguard against an extending cluster of dangers and progressively refined assaults inside the cloud climate including those that focus on the application level.[4]

THE REQUIREMENT FOR CLOUD APPLICATION SECURITY

Current venture responsibilities are spread across a wide assortment of cloud stages, going from set-ups of SaaS items like Google Work areas and Microsoft 365 to custom cloud-local applications stumbling into various hyper-scale cloud specialist co-ops.

Subsequently, network borders are more powerful than any other time, and basic information and jobs face dangers that just didn't exist 10 years prior. Undertakings should have the option to guarantee jobs are safeguarded anywhere they run. Furthermore, distributed computing adds another development to information sway and information administration that can confound consistency.[4]

Individual cloud specialist organizations frequently offer security answers for their foundation, yet in reality, as we know it, where multi-cloud is the standard—a Gartner review showed more than 80% of public cloud clients utilise different suppliers—arrangements that can safeguard a venture from start to finish across all stages are required.

CLOUD APPLICATION SECURITY DANGERS

- **Account commandeering:** Feeble passwords and information breaks frequently lead to genuine records being compromised. On the off chance that an assailant compromises a record, they can get to delicate information and totally control cloud resources.[5]
- **Certification openness:** A culmination of record capturing is qualification openness. As the Solar Winds security break illustrated, uncovering certifications in the cloud (GitHub for this situation) can prompt record seizing and an extensive variety of refined long haul assaults.
- **Bots and computerized assaults:** Bots and vindictive scanners are a sad truth of presenting any support of the Web. Accordingly, any cloud administration or web-confronting application should represent the dangers presented via robotized assaults.
- **Uncertain APIs:** APIs are one of the most widely recognized systems for sharing information both inside and remotely in current cloud conditions. Be that as it may, on the grounds that APIs are many times both element and information rich, they are a famous assault surface for programmers.[5]
- **Over sharing of information:** Cloud information capacity makes it insignificant to share information utilizing URLs. This enormously smoothes out big business cooperation. In any case, it additionally improves the probability of resources being gotten to by unapproved or vindictive clients.
- **DoS assaults:** Disavowal of Administration (DoS) assaults against enormous undertakings has been an online protection danger for quite a while. With such countless present day associations subject to public cloud administrations, assaults against cloud specialist co-ops can now have an outstanding effect.
- **Misconfiguration:** One of the most well-known purposes behind information breaks is misconfigurations. The recurrence of misconfigurations in the cloud is to a great extent because of the intricacy engaged with design the executives (which prompts disconnected manual cycles) and access control across cloud suppliers.[6]
- **Phishing and social designing:** Phishing and social designing assaults that exploit the human side of big business security are one of the most often taken advantage of assault vectors.
- **Intricacy and absence of perceivability:** In light of the fact that numerous venture conditions are multi-cloud, the intricacy of arrangement the board, granular observing across stages, and access control frequently lead to disconnected work processes that include manual design and breaking point perceivability which further compounds cloud security challenges.

CLOUD APPLICATION SECURITY BEST PRACTICES

Ventures should adopt an all-encompassing strategy to further develop their cloud security act. There's no one-size-fits-all approach that will work for each association, yet there are a few cloud application security best practices that all undertakings can apply. Here are the absolute most significant cloud application security best practices ventures ought to consider[7]:

- **Influence MFA:** Multifaceted confirmation (MFA) is one of the best systems for restricting the gamble of record split the difference.
- **Represent the human angle:** Client mistake is one of the most well-known reasons for information breaks. Adopting a two dimensional strategy of client instruction and carrying out security tooling, for

example, URL channels, hostile to malware, and keen firewalls can fundamentally decrease the gamble of social designing prompting a disastrous security issue.

• **Mechanize everything:** Undertakings ought to computerize cloud application observing, episode reaction, and setup however much as could reasonably be expected. Manual work processes are mistake inclined and a typical reason for oversight or spilled information.

• **Uphold the guideline of least honor:** Client records and applications ought to be arranged to just access the resources expected for their business capability. Security strategies ought to uphold the rule of least honor across all cloud stages. Utilizing endeavor character the board arrangements and SSO (single-sign-on) can assist undertakings with scaling this cloud application security best practice.

• **Utilize all encompassing multi-cloud arrangements:** Current undertaking foundation is perplexing and endeavors need total perceivability to guarantee serious areas of strength for a stance across all stages. This implies picking perceivability and security tooling that isn't intrinsically attached to a given area (for example point machines) or cloud seller is fundamental.

• **Try not to rely upon signature matching alone:** Numerous danger recognition motors and against malware arrangements rely upon signature coordinating and fundamental business rationale to distinguish pernicious way of behaving. While recognizing realized dangers is valuable, practically speaking relying just upon essential mark matching for danger location is a recipe for misleading up-sides that can prompt alarm weakness and pointlessly delayed down tasks. Moreover, dependence on signature planning alone means ventures have practically no insurance against zero-day dangers that don't as of now have a known mark. Security tooling that can examine conduct in-setting, for instance by utilizing an artificial intelligence motor, can both lessen bogus up-sides and decline the chances of a zero-day danger being taken advantage of.

TYPES OF CLOUD ENVIRONMENTS

When you're looking for cloud-based security, you'll find three main types of cloud environments to choose from. The top options on the market include public clouds, private clouds, and hybrid clouds. Each of these environments has different security concerns and benefits, so it's important to know the difference between them[6-8]:

1. Public clouds

Public cloud services are hosted by third-party cloud service providers. A company doesn't have to set up anything to use the cloud, since the provider handles it all. Usually, clients can access a provider's web services via web browsers. Security features, such as access control, identity management, and authentication, are crucial to public clouds.

2. Private clouds

Private clouds are typically more secure than public clouds, as they're usually dedicated to a single group or user and rely on that group or user's firewall. The isolated nature of these clouds helps them stay secure from outside attacks since they're only accessible by one organization. However, they still face security challenges from some threats, such as social engineering and breaches. These clouds can also be difficult to scale as your company's needs expand.

3. Hybrid clouds

Hybrid clouds combine the scalability of public clouds with the greater control over resources that private clouds offer. These clouds connect multiple environments, such as a private cloud and a public cloud, that can scale more easily based on demand. Successful hybrid clouds allow users to access all their environments in a single integrated content management platform.

CRYPTOGRAPHY

Changing over valuable information into indistinguishable text so no other person can peruse it with the exception of the pre-decided client is called encryption, and the procedures utilised are called cryptography strategies. It very well might be achieved through scrambling words, utilising code words, or utilising exceptionally effective numerical procedures. There are various calculations grouped into two groups: a. Symmetric Calculations: This calculation utilises the same key to encode and unscramble the message. For example, if some client needs to make an impression on another and wants no other individual to understand it, In this way, he can encode the information using a mystery key that can be imparted to the collector, who will unravel the information using a similar key[9]. As can be seen, judgement on the key has been imparted to every one of the clients who should recover information. b. Topsy-turvy Calculations: These sorts of calculations utilise two separate keys for decoding and encryption. A client figures out the information using one key (known as an open key), and the recipient unscrambles the message using a separate key (known as a confidential key). I. Public Key: This key is available all around the web and is used to encode the mysterious text. ii. Confidential Key: As the name implies, it is a recipient's confidential key, and only the collector will be able to utilise this key to unscramble the expected message.

DATA ENCRYPTION STANDARD (DES)

The reason this encryption technique is so popular is that it operates on bits. Fiesta structure is incorporated into this block cypher. The maximum length of a message that may be encrypted at once is 64 bits, while the key size is 64 bits. A check bit, which is eliminated when creating subkeys, is present every 7 bits. The procedures are as follows: i. Divide the plain text into left and right portions. ii. Create 16 subkeys, each with 48 bits of length. iii. Each 64-bit data block has a set of code words. As of right present, only the expensive and time-consuming brute-force method is known to be able to break through it, making it one of the best algorithms available[10].

ADVANCED ENCRYPTION STANDARD (AES)

AES also known as Rijndael structure is an iterative algorithm rather being called a fiestel structure. It also a block cipher has block capacity of 128 bits and key size any of 128, 192 or 256 bits. It is iterative because it uses rounds to convert data to cipher text depending on key sizes[9].

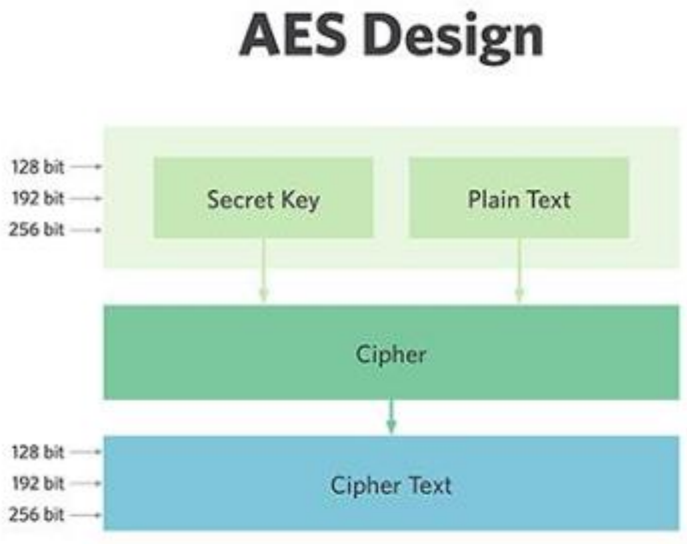

Figure 1: AES Design

CONCLUSION

With cloud computing, you can store and process data online with almost limitless infrastructure that requires very little upkeep and great scalability. It is clear that by using cryptographic techniques for safe processing, the ongoing vulnerability in the Cloud may still be addressed. By protecting data from unauthorized users via data encryption, security and data confidentiality can be achieved. Data can be encrypted by anybody using the public key; however, data can only be decrypted by those who possess the private key. When using hybrid encryption, each message's plaintext is encrypted to create a cipher text by the sender creating a new symmetric key. The public key of the recipient is wrapped in that symmetric key. Utilising RSA in the hybrid cryptosystem is also beneficial. A hybrid cryptosystem technique is employed to enhance data security. A file is secured using the symmetric algorithm in the hybrid cryptosystem, and the symmetric key is secured using the asymmetric algorithm. The suggested model made use of the fast-symmetric scheme and robust cryptosystem methods with less computational complexity, respectively, of the AES technique and its key encryption utilising ECC. The surety analysis of cloud data in a quantum computing environment will be the subject of future research.

REFERENCES

[1]. Orobosade, A., Favour-Bethy, T. A., Kayode, A. B., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. Communications on Applied Electronics, 7(33), 25-31.

[2]. Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 1-10.

[3]. Orobosade, A., Favour-Bethy, T. A., Kayode, A. B., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. Communications on Applied Electronics, 7(33), 25-31.

[4]. Kumar, L., & Badal, N. (2019, April). A review on hybrid encryption in cloud computing. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.

[5]. Ahmad, S. A., & Garko, A. B. (2019, December). Hybrid cryptography algorithms in cloud computing: A review. In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-6). IEEE.

[6]. Kumar, A., Jain, V., & Yadav, A. (2020, February). A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In 2020 international conference on power electronics & IoT applications in renewable energy and its control (PARC) (pp. 514-517). IEEE.

[7]. Abbas, M. S., Mahdi, S. S., & Hussien, S. A. (2020, April). Security improvement of cloud data using hybrid cryptography and steganography. In 2020 international conference on computer science and software engineering (CSASE) (pp. 123-127). IEEE.

[8]. Chaudhary, S., Suthar, F., & Joshi, N. K. (2020). Comparative study between cryptographic and hybrid techniques for implementation of security in cloud computing. Performance Management of Integrated Systems and its Applications in Software Engineering, 127-135.

[9]. Kaushik, S., & Patel, A. (2019, April). Secure cloud data using hybrid cryptographic scheme. In 2019 4th international conference on internet of things: smart innovation and usages (IoT-SIU) (pp. 1-6). IEEE.

[10]. Kaur, S., & Jain, L. (2020). A Hybrid Cryptographic Scheme for Improving Cloud Security Using ECC and TDES Algorithms. Current Journal of Applied Science and Technology, 39(47), 27-34.