International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03816
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Analysis of Modes of Data Security and Future Requirements for Cloud Based Storages

Gurpreet Singh [1], Ashoke kumar mahato [2]

1. Assistant professor, Department of Computer Science, St.Xavier's College, Ranchi.
2. Ex. H.O.D., Department of Mathematics and Ex. Dean of Science, D.S.P.M.U., Ranchi.

Abstract: Along with the advancements in technology, Cloud based storages are becoming a very popular method of data storage. With their growing popularity, concerns of security of data on clouds are also rising. At present, IaaS is the most commonly used deployment method of cloud computing. It requires capable enough encryption algorithms to safeguard the contents stored on cloud storages to prevent the malicious use of sensitive data.

Currently, identity based encryption (IBE), Data encryption standard (DES-256), Multi factor authentication (MFA) and Elliptic curve cryptography (ECC) are the most prominent methods of data security in cloud storages. In this paper, we are analyzing the working methods of these approaches and presenting a comparative study of them. Our objective is to find out the capabilities and shortcomings of these and further, we will examine the abilities and limits of these algorithms to meet the present requirements of data security.

Keywords: Cloud computing, IBE, MFA, ECC, DES-256, IaaS

1. Introduction

Cloud computing is becoming the most prominent mode of computing in modern era. As compared to conventional computing, cloud based computing approach offers a broad set of advantages which are making it a popular choice. Cloud computing is a way to deliver computing in the form of service instead of in the form of a product. In traditional approach, computing is delivered as a product where a user is required to purchase the software solution for computing requirement. Not only software, but hardware is also offered as a service through cloud approaches in many cases.

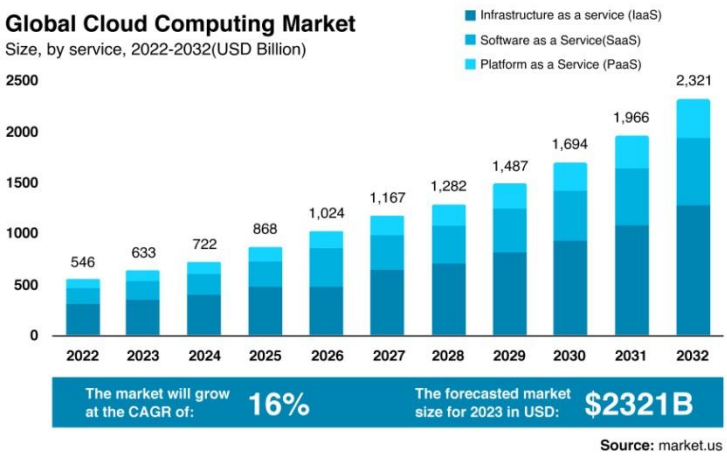
One of the most common scenarios in this regard can be seen in case of storage requirement. Conventional approach works by purchasing storage device in the form of a product that is most commonly a hard disk drive. It requires full payment for the device at once and further more the management of data contained in it also to be handled by the user. On the other hand, cloud oriented approach offers network based online storage device that can be used in the form of service. User is required to upload the data on the online drive and a convenient interface is also offered by the provider to do that. It makes cloud based approach easy to use and more manageable. Another advantage is that, user need not to pay at once for the whole storage, instead, user is required to pay only the amount that is calculated on the basis of use and time of usage.

2. Data analysis and literature review

Majority of the providers are offering a large part of such network based storage free of cost that can be used without paying. For an instance, leading information technology organization, Google offers online storage named Google Drive with 15GB of space free of cost. When we compare it the cost of 15GB hard disk drive based storage, we will understand the benefits of cloud computing over conventional

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI: 10.55041/ISJEM03816
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

computing. Due to such advantages in terms of economy and convenience in terms of technical usability, cloud computing is becoming most prominent choice of computing. We can observe and understand the growing popularity of Cloud computing during the recent years and the prediction about the growing market of it for the coming years.[1]



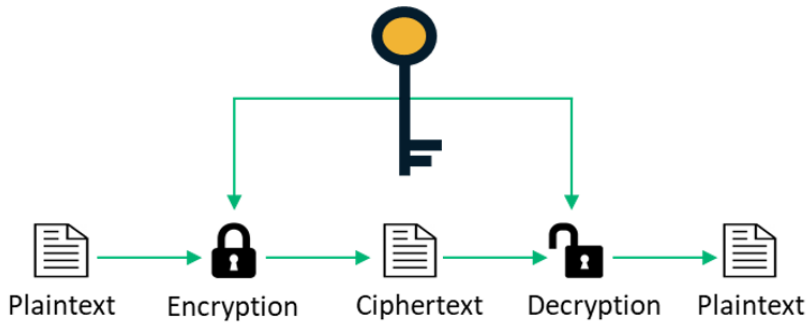
In this statistical represnetation, cloud statistics are provided from year 2022 and the predictions are made till 2032. Here we can clearly see that PaaS (Platform as a Service) is the fastest growing option of Cloud oriented computing. Its market value is expected to reach up to $2321 Billion till 2032.

However, along with the growing popularity of this newer approach of cloud computing, the challenges in its pathway are also increasing with the same pace. Most commonly seen shortcoming associated with this approach of computing is security and privacy of data. It is simple to understand that when personal data belonging to users is stored in network based storages, the risk of its unauthorized access and its theft is always a possibility. However, to overcome this problem, service providers are offering newer and newer modes of data encryption to enforce security of it. Here, in this paper we are going to deeply analyze different methods of data security.

To name a few, they are DES-256(Data Encryption Standard-256), Multi factor authentication (MFA) and Elliptic curve cryptography (ECC) used by leading cloud service providers at present. These methods are known to be the prominent modes of data security used in cloud based data storages. After analysis, we will analyze the future prospects and further requirements to strengthen these to face the challenges of coming epoch in the growing field of cloud computing.

3. Current means and methods

First, it should be understood that any traditional encryption system works by taking plaintext, i.e. the data to be encrypted. This plaintext is passed through the steps of encryption algorithm to transform it into cipher text. Now, this cipher text is understandable in encrypted form and hence it is considered to be safe and secured when stored somewhere or being transmitted across a network. Further, when this cipher text is accessed be some authentic user, it is passed through the steps of decryption algorithm as it is assumed that authentic user maintains hisown copy of decryption algorithm. This way the data is decrypted and then used for its purpose. The procedure can be understood with the help of this representation [2].



The shortcoming associated with this approach is, when a copy of steps of encryption and decryption algorithm is somehow obtained by malicious attackers, the data can be decrypted and security system fails. This way the end to end

encryption of data cannot be always enforced. Newer security algorithms struggle to address this issue and they attempt to encrypt the data in such a way that the steps of encryption and decryption, i.e. the key also remains like a unique possession with the authentic user of the data. The first approach in this regard is DES-256.4

DES-256, i.e Data Encryption Standard, works by using same key to encrypt and decrypt the data and due to this, the key must be known by the sender and the receiver or in our case, the user who is storing the data.

DES uses block cipher that is a cryptographic key to apply on a block of data at once. DES arranges the data to be encrypted into 64 bits blocks and each block is encrypted using the secret key into a 64 bit cipher text by using methods of mathematical permutations and substitutions. Further, it encrypts the data in different ways like encrypting each block independently or encrypting the blocks as a series of encryption i.e. by defining and maintaining relations and dependency between them. Additionally, DES uses a lengthy 64 bit key in which 8 bits are used for parity check and error detection and remaining 56 bits work as effective key for encryption. DES also provides backward compatibility in some cases.

Despite being enough capable and based upon strong logic of data encryption, this method suffers from the problem of unauthentic possession of the key which can be used to access the data in a malicious way. Further, it is also sensitive to brute force attack that means applying every key on the data until a match is found. This way the DES is considered to be ineffective at present but by using its logics and methods as a guide map, another encryption algorithm AES (Advance Encryption Standard) is developed which is able to address its shortcomings up to a great extent. AES works by dividing data into 128 bit size that is much larger as compared to 64 bit size of DES blocks. It is considered fully secured due to its robust working and strong system of data encryption. Key length used by AES can be 128, 192 or even 256 bits that is able to provide highly complex form of encrypted data and that is nearly impossible to break with brute force attacks. Process of encryption of data can be summarized by expressing the

The AES algorithm operates on a 128-bit block of data. Encryption process is executed for Nr - 1 loop times. Here, each loop is called as a round and the number of iterations in a loop, Nr can be 10, 12, or 14. Actual value of Nr depends upon the key length. As stated above,The key length can be 128, 192 or 256 bits in length respectively. The first and last round differ from other rounds because in that there is an additional Add Round Key transformation at the start of the 1st round and also Mix Column operation is not performed in the last round [2]. Explaination of AES encryption process with example is an extremely lengthy procedure and beyond the scope of our comparative study.

4. Conclusion

Here we can see that the security of data stored in clouds is the most important aspect of cloud computing that is needed to be addressed. This is because among cloud deployments, public cloud allows restriction free access to the stored data. At present, mostly symmetric cryptography based processes are used to encrypt data in cloud based storages. DES-256 was used earlier to encrypt data but it is not considered suitable for clouds as it is sensitive to hit and trial breach attempt which is termed as brute force attacks. To overcome this issue AES is developed which is considered much more secured and safe as compared to DES. However, it solves the problem of external malicious access attempts up to a great extent but at present many more security breach issues are needed to be addressed.

References:

1. https://appstekcorp.com/blog/top-6-cloud-computing-trends-for-2023/
2. https://ieeexplore.ieee.org/document/7830066
3. L. Ertaul, S. Singhal & G. Saldamli, Security Challenges In Cloud computing
4. R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing
5. Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).
6. Mondal, S.K., Pan, R., Kabir, H.D., Tian, T. and Dai, H.N. (2022) Kubernetes in IT Administration and Serverless Computing: An Empirical Study and Research Challenges. The Journal of Supercomputing, 78, 1-51.