INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 04 ISSUE: 09 | SEPT -2020 ISSN: 2582-3930

Data Security in cloud service providers- a Comparison of different cryptographic methods

Sudha D
Assistant Professor, Department of MCA
SCMS School of Technology and Management, Aluva ,India

Abstract --- In this current era of computer science, cryptography is for securing information and communication techniques and algorithms to transfer messages in way that are hard to decipher. Cryptosystems refer to mathematical procedures and computer programs. Now-a-days cloud computing is showing consistent growth in the field of computing. With the help of cloud and cryptography new era has begun in the field of technology. So that its easy to build privacy preserving storage model where data sharing services can update and control the access and limit the usage of their shared data. Preserving privacy is an important issue for cloud computing and it needs to be considered at every phase of design. This paper gives an idea on how the data is stored in cloud how they are secured and managed in cloud with the example of different platforms such as Google cloud , Azure and AWS.

Index Terms— Cryptography in Cloud, Client side Encryption, Server side Encryption, Key storage, cloud computing, meta data .

I. INTRODUCTION

Cryptography is the art of extreme information security. Better the cryptographic algorithm used security remains high. As cryptography is good, the message will remain secure. Cryptographic algorithms that take input data, called plaintext, and produce scrambled output . Scrambling, used in this sense, is much more than just moving letters around or exchanging some letters for others. After applying proper cryptographic algorithms, the output is typically in differentiate from a random string of data. Many cryptographic algorithms are reversible by knowing a particular secretket. Firstly in this paper we give a detail description about cryptography and its uses.

Section two gives us an idea about the clouds and its security systems. Cloud computing is one of the popular topics of the current world. Internet has started driving all these new technologies. Internet was designed firstly to be strong, but not completely safe. There are many data privacy concerns in cloud computing. Incorrect revelation of a data used in businesses in cloud to third parties is one of the major issues that has been found[4]. It contains a pool of computing resources that are accessed by the cloud users through Internet. The major benefits of using cloud are scalability, flexibility, efficient communication, reduced time and cost. A framework that can be followed easily to share the file which residing on the cloud with another cloud user. In this a concept of cryptography has been used to generate the secure key that can be shared among users.

In cloud computing integrity and privacy is very important. In the next section propose a study on how these techniques are applied in different platform. Gives separately how in client side and server side encryption are done. Their types subdivision are also mentioned clearly. The concept defined are almost same how they are implemented is different in different platforms. Algorithm used in these platform how they gives security, how data is manipulated and stored. For each platform they provide slit difference in the storage mechanism.

Section V gives full detail about the three different platforms I mentioned above. Section VI gives the difference between different platforms. The last section gives the future scope and conclusion about this paper. The reference section helped me in developing this paper successfully.

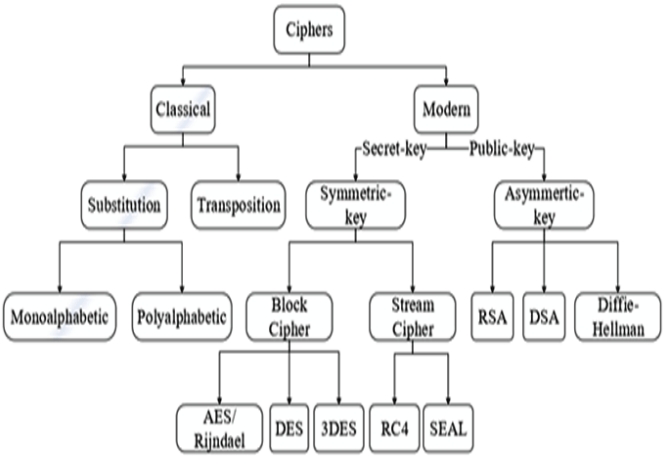
II. CRYPTOGRAPHY AND ITS NEEDS

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party. There are following two types of algorithms such as: (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key

algorithm. Symmetric algorithm can be further divided into two types.

Various cryptanalysis techniques are available to break most of the encryption algorithms at any time. Lot more algorithms are broken at different stages by eavesdroppers. Algorithms like block cipher or stream cipher or any other cipher types could be easily attacked by various cryptanalysis techniques. A brute force attack, linear and non-linear cryptanalysis, meet in the middle attack, man in the middle attack, and etc., are few to name.

Cryptography provides confidentiality, integrity, authentication and nonrepudiation of data. On the basis of key, there are two types of cryptographic schemes available. They are Symmetric and Asymmetric-key cryptography. These two types serve the purpose of confidentiality. The keys involved in symmetric key algorithm are identical for both data encryption and decryption. The users must choose the keys more carefully and the keys are securely distributed and stored. On the contrary, the asymmetric cryptography uses two mathematically linked distinct keys. Unlike in symmetric-key cryptography, plaintext and cipher-text are treated as integers in asymmetric-key cryptography [13].



A. Key Generation

The cryptographic systems in modern technology include symmetric-key algorithms (such as DES and AES) and public key algorithms (such as RSA). The user encrypts the data with the public key. Only the provider of the private key decrypts this data. The simplest method to read encrypted data is a brute force attack, meaning just attempting every number, up to the maximum length of the key. Therefore, it is important to use sufficiently longer key length since longer keys take longer time to attack, resulting brute force attack almost impractical.

B. Key Storage

The keys must be stored securely to maintain the security in the process of communications. There are various techniques in use for this purpose. The most common technique is that an encryption application manages to keep the keys for the user and it depends on an access password to control the use of the key.

C. Key Usage

The length of the key use is the major issue. The keys must be frequently changed as the required efforts of the attackers are on the increase. The frequent change in key also limits the loss of information. The frequency of usage decreases as the frequency of key change increases. This happens especially when the attacker tries to trace the keys. Symmetric keys have been used for longer times since key exchange has become a difficult process. The symmetric keys must change with every data or interaction, so that only the intended data will become accessible eve n if the key is stolen, cryptanalyzed, or socially engineered.[1]

III. IMPLEMENTATION OF CLOUD

Cloud is one of the widely used technology due to its efficient infrastructure and deployment model. It contains a pool of computing resources that are accessed by the cloud users through Internet.[14] The major benefits of using cloud are scalability, flexibility, efficient communication, reduced time and cost. Providing security to cloud is the demanding task for enabling a secure storage and access of the data.

In cloud computing, Data sharing is an essential aspect for secure, efficient and flexible sharing of data with the other authorized users. New public-key cryptosystems produce Coded texts which are of constant size so that decryption rights for sets of Coded texts can be efficiently secret keys which are aggregated. The user who possesses the secret key is allowed to release a constant-size aggregate key so that Coded text set can be flexibly chosen while ensuring that the other encrypted files out of the set stay confidential.[12][7]

Figure :Basic cloud computing

Cloud Computing provides three kinds of services:0

i) Private cloud: This type of cloud owned by the organization is meant to provide services to its own users.

ii) Public cloud: Third party are providing the services. Examples include Amazon Web Services (AWS), Microsoft Azure, IBM/SoftLayer and Google Compute Engine.

iii) Hybrid cloud: This is a combination of services provided by private and public clouds. The main goal of this kind is to achieve scalability.

IV. LAYERS AND SECURITY ISSUES IN CLOUD

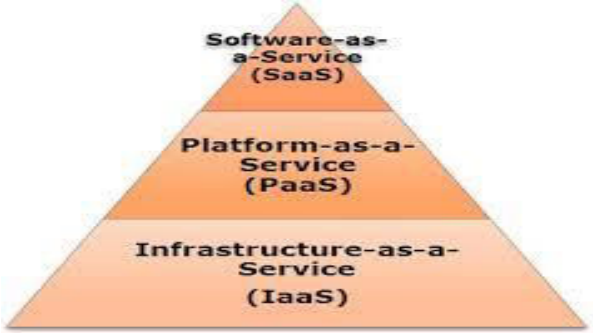
Cloud computing has three categories of services:

i) Infrastructure as a service: It helps users to transfer work from one machine to another, usually a virtual machine.

ii) Platform as a Service: PaaS is used for general software development. Common PaaS providers include Salesforce.com's , Force.com, Amazon Elastic Beanstalk, and Google App Engine.

iii) Software as a service: SaaS delivers software applications over the Internet; these are often called Web Services. Microsoft Office 365 is an example of an SaaS. [2]

Cloud computing seems really simple to the consumers of cloud as in access cloud, place or retrieves required data that's all. But the internal cloud is built on three very important layers.[11] Those layers are named as software as a service (SaaS), Platform as a service (Paas) and Infrastructure as a service (IaaS). Various cloud service providers provide different kind of services based on those layers. On the first level that is software as services, various applications reside that provides an interface to end users. This layer generally allows access to internal data with some authentication mechanism. The second layer is a platform as a service, this layer contains various mappings of users request to the required resource that resides on cloud computing. At last there is infrastructure layer that is most time contains virtual machines and infrastructure that user can request for computations. Each layer of cloud contains its own vulnerabilities. Like software as a service, layer uses authentication mechanism to validate owner's identity on the document, but this can be broken if someone possess security code that is being used for authentication.



V. PLATFORMS

A. AMAZON WEB SERVICES

AWS provides multiple services to help you protect your data at rest or in transit. the cloud services provided by Amazon, known as Amazon Web Services (AWS), has gained special attention over the past few years. AWS- AWS is a cloud service provider, which is an illustration of accurate cloud computing that offers cloud services and keeps the user data confidential, secured and available. It is the provider of on demand services and the user has to pay for only the resources he uses. Data is at the core of business today, and data encryption offers a solid way to make sure that data stays secure. As one of the most popular storage services on AWS, Amazon S3 has several encryption methods available.[8][9]

AWS has several offerings in the data encryption space. In addition to the Amazon S3 encryption offerings discussed here, Amazon Elastic Block Store (AWS EBS) encryption options are also available.

- ***SSE Data Encryption***

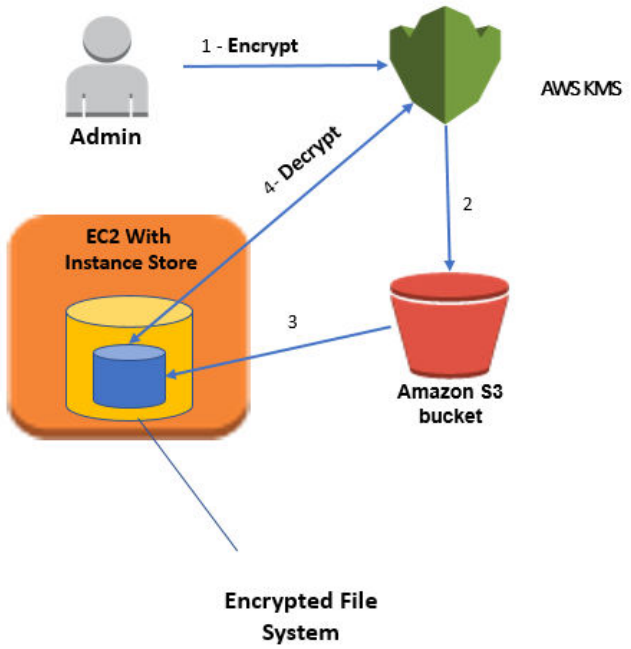
Within Amazon S3, Server Side Encryption (SSE) is the simplest data encryption option available. SSE encryption manages the heavy lifting of encryption on the AWS side, and falls into two types: SSE-S3 and SSE-C.The SSE-S3 option lets AWS manage the key for you, which requires that you trust them with that information. With SSE-S3, you don't have access to see or encrypt data using the key directly, but you can be assured that the raw data you own is encrypted at rest by AWS's standard processes.The SSE-C option similarly manages encryption and decryption of your data for you, but uses a key provided by you (the customer) and passed in to

AWS with each request to encrypt or decrypt. AWS does not store your key with this method, so you are responsible for its safe keeping.

- ***CSE Data Encryption***

S3 Client-Side Encryption puts all the responsibility for the encryption heavy lifting onto the user. Rather than allowing AWS to encrypt your data, you perform the encryption within your own data center and upload the encrypted data directly to AWS. S3 Client-Side Encryption also comes in two options: server-side master key storage, and client-side master key storage. In server-side master key storage, you can store your master key server-side in the AWS KMS (Key Management Service) service, and AWS will provide sophisticated key management software to manage sub-keys based on the master key that is used to encrypt your data. In client-side master key storage, your master keys aren't stored on AWS's servers, and you take full responsibility for the encryption. Using this second approach is potentially the most secure, as your keys and data are never seen by Amazon servers in an unencrypted state. However, the level of security that you can achieve with this method depends on the integrity of your own processes and technology rather than AWS's.

Architectural Overview



In this architectural diagram:

1. The administrator encrypts a secret password by using KMS. The encrypted password is stored in a file.
2. The administrator puts the file containing the encrypted password in an S3 bucket.
3. At instance boot time, the instance copies the encrypted file to an internal disk.

- ***AWS Services***

1. AWS Key Management Service (KMS)-- AWS KMS is a managed service that enables easy creation and control of encryption keys used to encrypt data. KMS uses envelope encryption in which data is encrypted using a data key that is then encrypted using a master key. Master keys can also be used to encrypt and decrypt up to 4 kilobytes of data. In our solution, I use KMS encrypt/decrypt APIs to encrypt the encrypted file system's password
2. AWS CloudTrail -- CloudTrail records AWS API calls for your account. KMS and CloudTrail are fully integrated, which means CloudTrail logs each request to and from KMS for future auditing. This post's solution enables CloudTrail for monitoring and audit
3. Amazon S3 – S3 is an AWS storage I use S3 in this post to save the encrypted file system password.
4. AWS Identity and Access Management -- AWS IAM enables you to control access securely to AWS services. In this post, I configure and attach a policy to EC2 instances that allows access to the S3 bucket to read the encrypted password file and to KMS to decrypt the file system password.

B. GOOGLE CLOUD

Google uses several layers of encryption to protect customer data at rest in Google Cloud Platform products. Google Cloud Platform encrypts customer content stored at rest, without any action required from the customer, using one or more encryption mechanisms. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys that are exclusively stored and used inside Google's central Key Management Service. Google's Key Management Service is redundant and globally distributed. Data stored in Google Cloud Platform is encrypted at the storage level using either AES256 or AES128. Google uses a common cryptographic library, Tink, to implement encryption consistently across almost all Google Cloud Platform products. Because this common library is widely accessible, only a small team of cryptographers needs to properly implement and maintain this tightly controlled and reviewed code.

For many individuals and companies, security is a deciding factor in choosing a public cloud vendor. At Google, security is of the utmost importance. We take security and privacy seriously, and we work tirelessly to protect your data —

whether it is traveling over the Internet, moving between our data centers , or stored on our servers. Central to our comprehensive security strategy is encryption in transit and at rest, which ensures the data can be accessed only by the authorized roles and services with audited access to the encryption keys. This paper describes Google's approach to encryption at rest for the Google Cloud Platform, and how Google uses it to keep your information more secure. This document is targeted at CISOs and security operations teams currently using or considering using Google Cloud Platform. With the exception of the introduction, this document assumes a basic understanding of encryption and cryptographic primitives.[10]

Google Refine or Open Refine is a free and powerful tool for cleaning, reconciling and transforming messy and unstructured data. It is a web-based application, therefore, the datasets can be linked and extended with the external data and various web services. Many web services also allow Google Refine to upload cleaned data to a central database. Google uses several layers of encryption to protect customer data at rest in Google Cloud Platform products. Data for storage are split into chunks and further encryption are done. Data are entered by the customers through their account. Customer data includes (i)contents (ii)metadata. Also key management plays an important role here.

Google uses several layers of encryption to protect data. Using multiple layers of encryption adds redundant data protection and allows us to select the optimal approach based on application requirements. Several layers of encryption are used to protect data stored in Google Cloud Platform. Either

distributed file system encryption or database and file storage encryption is in place for almost all files; and storage device encryption is in place for almost all files. Google uses the Advanced Encryption Standard (AES) algorithm to encrypt data at rest. AES is widely used because both AES256 and AES128 are recommended by the National Institute of Standards and Technology (NIST) for long-term storage use (as of March 2019), and AES is often included as part of customer compliance requirements.

C. MICROSOFT AZURE

Microsoft Azure is a flexible cloud platform that allows fast development, debugging and iteration of the applications, as well as their further management through a network of Microsoft data centers.[5] Applications can be developed with any tool, programming language, or existing framework, while there is possibility of integrating public cloud applications with existing IT environment. To subscribe to the Azure, it is necessary to use some of the Microsoft Live accounts (Live, Hotmail, Outlook) and credit card. After completing the registration the user can make the purchase of needed resources in the cloud. VMs generation is performed from a management console, with the possibility of selecting different options among the list of those that are available.[15]

Azure is a foundation for fleeing data in the cloud. Instead of giving programming that Microsoft customers can present and run themselves in solitude PCs. Nowadays, Azure is an association: Customers utilize it to sprint apps and stockpile facts & figures on web-accessible devices rued by Microsoft Corporation. Azure Platform is a web-based distributed technology. Extremely systematic, changeable and compatible capacity can be utilized to a mass unused apps to remain constant.

Components of window's azure : i]Computer: Windows procedure can run a gathering of vocations. Whatever an application does, regardless, it needs to be done as no short of what one occupation. Azure at that factor typically runs a variety of examples of each movement, utilizing worked in load changing as per spread needs crosswise over them. ii] Storage: The 2nd stage in Azure is a limit. We have three journalists perfect here – Blobs, that take after records, Tables, which are entered and well-shaped limit, and lines, which let Web Parts and Specialist Parts, provide for one another. iii] Fabric Controller: The 3rd sort out in Azure is the connect controller or App connect. It handles articulations and association – between Microsoft Windows Azure applications, and in development from the servers. Ready to express that we got the opportunity to have that expansive SQL Server or Database structure and enabling access to an Azure app, & we will not permit customers of an app in our framework.

VI. COMPARITIVE STUDY

	AWS	AZURE	GOOGLE
YEAR (officially)	**2006**	**2011**	**2008**
TECHNOLOGY	**EC2 Service**	**Virtual Machine**	**Computer Engine**
STORAGE	**S3** **EFS** **EBD**	**Blob Storage** **File Storage** **Disk**	**Cloud Storage** **Persistent Disk**

		Storage	
DATA WAREHOUSE	**Aurora** **RDS** **RedShift**	**Data Lake Store** **SQL Database** **Table Storage**	**Cloud Datastore** **Cloud SQL** **Cloud Bigtable**
KEY CLOUD TOOLS	**Athena** **Lex** **Deep lens**	**Data factory** **Bot Service** **Functions**	**Big Query** **Cloud Dataflow** **Cloud Functions**
INTERNET OF THINGS	**IoT Greengrass**	**IoT Hub**	**Cloud IoT core**

VII. FUTURE SCOPE

The next era of cryptography lies in associated with the key used for encryption and decryption purpose. There is some many advantages and disadvantages for the use of key. As the new technologies come to play security issues are solved to a large extend .

Another way that overcome the threats of key is by using unclonable key. It simply means cryptography without using secret key. Most security applications, for instance, access to buildings or digital signatures, use cryptographic keys that must at all costs be kept secret. Using a physical unclonable key (PUK) – which can be a stroke of white paint on a surface – and the quantum properties of light.

VIII. CONCLUSION

All the platforms mentioned above offer rich set of features and the selection between them is a factor of the user needs. This study help us to get a detailed idea about the different platforms, how each parts of encryption, storage, manipulation works. As a review all the platform have their own signature in different and unique way but the basic is same in all the platform.

With the help of cryptography the cloud technology come to most secured and privacy one. Different algorithms are implemented in every stage of cloud system for improving the level of security.

IX. REFERENCE

[1] Aciobanitei, I. (2018). *A Cryptography API: Next Generation Key Storage Provider for Cryptography in the Cloud.* ECAI.

[2] Alqahtani, A. (2018). *Cloud Computing and Security Issues—A Review of Amazon Web Services.* International Journal of Applied Engineering Research.

[3] Arif, H. (2019). *A Comparison between Google Cloud Service and iCloud* . ieee.

[4] Chatterjee, R. (2017). *Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud* .

[5] Dordevic, B. S. (2014). *Cloud Computing in Amazon and Microsoft Azure platforms: performance and service comparison* . TELFOR.

[6] GUPTA, A. (2020). *Implementation of Storage in Virtual Private Cloud using Simple Storage Service on AWS* .

[7] Iyengar, A. (2018). *Enhanced Clients for Data Stores and Cloud Services.* ieee.

[8] Kaur, A. (2018). *Performance Evaluation of AWS and IBM Cloud Platforms for Security Mechanism* . ieee.

[9] Kotas, C. (2018). *A Comparison of Amazon Web Services and Microsoft Azure Cloud Platforms for High Performance Computing* . IEEE.

[10] Naik, N. (2016). *Connecting Google Cloud System with Organizational Systems for Effortless Data Analysis by Anyone, Anytime, Anywhere.*

[11] Pol, P. (2016). *SECURED CLOUD DATA SHARING USING AUDITABLE AGGREGATE KEY.* IEEE.

[12] S, S. K. (2013). *A Secure and Efficient Way of Accessing Encrypted Cloud Databases Using Adaptive Encryption Scheme.* IJSR.

[13] Selvanayagam, J. (2018). *SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY* . IRJET.

[14] Thangapandiyan, M. (2018). *Quantum Key Distribution and Cryptography Mechanisms for Cloud Data Security.* International Conference on Communication and Signal Processing.

[15] Verma, A. (2019). *A Detailed Study of Azure Platform & Its Cognitive Services.*