IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 9, September 2020

DOI 10.17148/IJARCCE.2020.9916

Literature Survey on Cloud Cryptography for Data Security

Jyoti Gangesh Tiwari[1], Gayatri Sanjay Chavan[2]

Computer Science and Engineering, Navrachana University, Vadodara, India[1,2]

Abstract: During this paper we have a tendency to square measure reaching to discuss concerning completely different technologies that square measure employed in cryptography technique, Cloud Cryptography is one amongst the vital facet within the world of knowledge security. It includes completely different encoding and secret writing techniques that square measure want to keep our Data safe and secure on cloud. In Cloud Cryptography we have a tendency to use public and personal keys for Encrypting and Decrypting Data to keep up the integrity of knowledge. The quality with that cloud computing manages Data secrecy, and data security makes the market hesitant concerning cloud computing thus, during this paper we are going to discuss this parameter conjointly to clear the professionals of the cloud cryptography.

Keywords: Cloud Security, cryptographic algorithm, security infrastructure, Hybrid cloud.

I. INTRODUCTION

According to Nist definition "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing may be a platform for increasing capabilities and developing potentialities dynamically while not using new infrastructure, personnel, or computer code systems. additionally, cloud computing originated from a poster enterprise idea, and developed into a flourishing IT invention. Cloud cryptography is nothing however the technique for keeping our knowledge safe and secure from the third-party, As when applying the cryptologic techniques our knowledge is regenerate into non- decipherable kind in order that nobody except sender and receiver will scan or build any amendment in knowledge.

There are two types of cryptographic techniques which are used to keep our data secure from unauthorized party i.e1] Symmetric key based algorithm , 2]Asymmetric key based algorithm. It is very important to keep our data safe from the malicious attack .As our data is on cloud with the help of internet different unauthorized party can (secure) our data Security brings different concerns with it like integrity, availability and confidentiality. Data integrity and availability suffers due to failure of cloud service. The new idea is getting used today i.e CaaS (Crypto as a Service) this has brought the idea of cloud computing from the facet of data security, it finds the new approach for the appliance of the cryptography technology within the cloud surroundings and conjointly permits us to pioneer new technique. As we can see in Fig 1 that in cryptography we use two types of key public and private for encryption and decryption and further that keys are being biffurcated into different techniques according to its uses i.e RSA technique which use public key and private key is used in block cipher and stream cipher further if we see block cipher has many techniques like RC2, AES,DES,3DE,RC6,Blowfish etc.these are some of the famous technique used for cryptography.

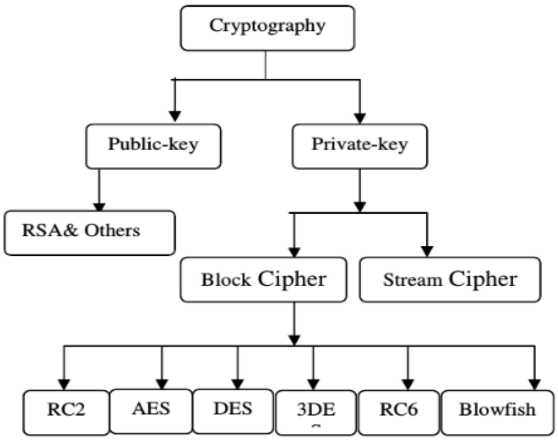

Fig 1: Diagram of categorization of different cryptographic techniques.

DOI 10.17148/IJARCCE.2020.9916

II. ENCRYPTION

It is the method of cryptography the information into ciphertext from plaintext in order that no third party will scan or amendment it. Ideally solely the licensed individuals will decipher or decipher the text as a result of encoding uses completely different key connected algorithmic program which secret is solely with the sender and receiver .The one who is aware of the decrypting technique are going to be allowed to access the first info. It helps to provide security for sensitive information. Three types of encryption are used now a days one is symmetric and other is Asymmetric encryption and Hashing. There are five main components of Symmetric Encryption that are: plain text, encryption algorithm, cipher text, secret key and decryption algorithm. Here is some famous encryption algorithm which are:

1) RC4: it's one amongst the quickest encoding algorithmic program, its key-size is from 40-bit to 1024-bit.
2) Triple DES: This algorithmic program was designed to interchange the first encoding customary as a result of hackers learned to simply crack it. Triple DES uses 3 individual keys of 56-bits every. As Triple DES remains a dependable hardware encoding resolution it's slowly being phased out.
3) RSA Encryption: It is public-key encryption algorithm and now it has also become a standard for encryption data senover internet. It is also known as the asymmetric encryption algorithm because it uses pair of keys. One is public-key for encryption and the private –key is for decryption.
4) AES: Advance Encryption Algorithm it is declared as the standard encryption by the U.S government and many other organizations. It also uses keys 192 and 256 bits for heavy –duty encryption.

III. HASHING

Hashing is also one of the technique to secure your data on cloud. It is a function which generate a fixed length result, which is also called hash-value or hash. It is a mathematical algorithm that maps data of arbitrary size to a hash of fixed size. Hash functions are used for Digital signatures, Message Authentication Code and other form of authentication. There are two main types of Hashing techniques which are MD5, SHA. Hash functions are also used to build caches for large data sets stored in slow media. A cache is generally simpler than a hashed search table, since any collision can be resolved by discarding or writing back the older of the two colliding items. The efficiency of mapping depends of the efficiency of the hash function used.

MD5*:* The Message-Digest hashing algorithm is hash function producing a 128-bit hash value. The input message in this is divided into chunk of 512 bits blocks. The processing of message takes place in four different stages i.e termed as “Round” and each round have 16 similar operations.

SHA*:* The Secure Hash Algorithm are the part of cryptographic hash functions. There are different versions of SHA algorithm some of the examples are SHA-0, SHA-1, SHA-2, SHA-3.

a) SHA: It is the original version of 160-bit hash function but it was withdrawn very soon because of some significant flaw and replaced by SHA-1.
b) SHA-1: It is also a 160-bit hash function which resembles the MD5. This was designed by National Security Agency (NSA) so that it can become a part of Digital Signature Algorithm. Some cryptographic issues were reported in this algorithm so it was not approved mostly after 2010.
c) SHA-2: It is the different version of SHA family as it consists of two similar hash function but with different block size known as SHA-256 and SHA-512, they differ in word-size SHA-256 uses 32-byte words and SHA-512 uses 64-byte words.
d) SHA-3: It is also called as “keccak”, It supports the same length as SHA-2 just the difference is that its internal structure varies from all other SHA-family.

IV. DIGITAL SIGNATURES

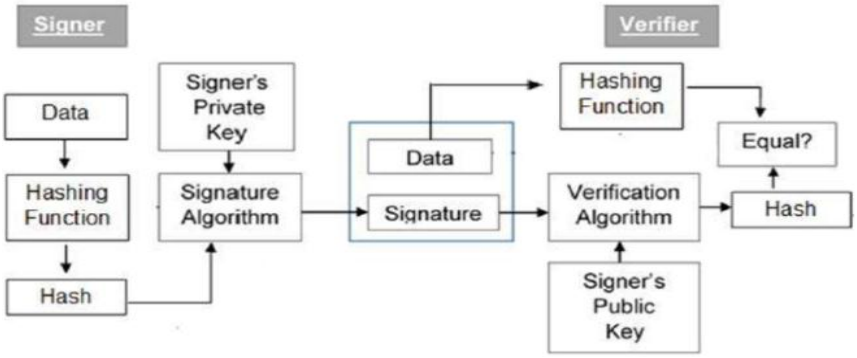

Fig. 2 A simple example diagram of digital signature.

Digital signatures are used to validate the authenticity and integrity. It is a mathematical technique that binds the identity of a person to the digital data, it is one of the primitives of public-key. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. In Fig 2 it is shown how the digital signature is used for the cryptographic process. In this process there will only be the signer and verifier and data will only be encrypted if the receiver party has the proper signature of sender. In this we use hashing also at both the end to get our data safely and securely.

V. LITERATURE SURVEY

In this section we will discuss about all the literature survey which we have done regarding this topic.

In 2018 Joseph Selvanayagam wrote a paper titled Secure File Storage on Cloud using Cryptography.[1] The aim of this paper is to understand about the security threat of stored File on cloud using different techniques of cryptography. In this paper author has described about the Asymetric and symmetric techniques which is one of the famous encryption and decryption techniques. In this AES and DES techniques has been described in detail , All the steps of both the techniques is been discussed in this paper . One more technique which is discussed here is RC-2 Encryption Algorithm.

In 2018 Bin-hwaang Lee wrote a paper titled Data security in cloud computing using AES [2]. In this paper they have discussed about the security threats and identify the appropriate security techniques used to mitigate them in cloud computing . In this paper they had discussed about data security in cloud computing using AES under HEROKU cloud, After that the implemented a website as an application for data security and in AES they implemented AES as data security algorithm.

S. Lei in his paper named Research and Design of Cryptography Cloud framework[3] had discussed about different frameworks of how cryptography is done in cloud computing .In this they have also discussed in detail how public and private key is used for encryption and decryption purpose and even they had talk about virtualization cryptoraphy machine(VCM) and its work flow that how different techniques is being used for making cloud computing safe and secure. This is one of the research paper in which each and every flow, architecture has been mentioned about cloud cryptography, they have mentioned much about virtual cryptography machine(VCM). Which is one of the cryptography service provider. In this they also proposed the framework for CC which shows that ther are going to provide cryptographic services with cloud computing model to consumers.

Ahmad.S.A in his paper “Hybrid Cryptography Algorithm in cloud computing”[4] had discussed about the hybrid approach i.e instead of one encryption method he merged two different encryption methods so thtah they can provide more security to data , as we can see that one encryption algorithm is easy to crack but if we use two encryption algorithm then it will be difficult for any third party to decrypt. This is one of the innovative approach as malfunction of data increasing day by day we can secure our data by this hybrid approach. In his review paper he had also discussed about different approaches of different researchers so that we can get better idea for cryptography algorithms. The comparison made in this paper can clearly say about the different hybrid approaches.

Pandey.s proposed a paper titled Data Security in Cloud-Based Applications. [5] in this paper he had discussed about the security challenges which we are facing regarding the security. And for overcoming that issue he suggested the AES technique. AES is a one type of block cipher technique which uses private key for the security purpose. In this paper he had mentioned all the steps of AES technique. In this he had also discussed about the three security patterns i.e. filtering, encryption, permission for providing right data security.

In 2017 sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). [6] This technique provides a mutual trust for both cloud users and cloud service provider to avoid security related issues in cloud computing. The aim of this paper is to propose a system which include EMTACA algorithm which can enhance guaranteed and trusted and reputation-based cloud services among the users in a cloud environment the result of this paper showed data confidentiality, integrity, availability which is three most important aspect of data security was achieved.

VI. CONCLUSION

In this we surveyed different cryptographic techniques and its main components on which the whole process of cryptography is carried out. There are many difficulties also in carrying out different techniques but one or another techniques overcome the issues of threats. In this paper we even discussed about different areas and sub techniques of cryptographic techniques. One of the main aspects of this survey was to get different ideas for securing our data in cloud.

Even we discussed about cloud framework and cloud platforms which provides services and security. This paper is gving the survey of current publication in the aspect of cloud cryptography and data storage that can assist researchers through their fields and select cryptographic algorithm for their research. In this paper it's the limited amount of cryptographic algorithms dicussed but a sample of papers discussed are showing the benefits and constraint of used cryptographic algorithm which are aimed to provide more and more information regarding this topic.

REFERENCES

[1]. Joseph Selvanayagam1, Akash Singh2, Joans Michael ,Jaya Jeswani,Secure File Storage on cloud using cryptography: (IRJET),2018

[2]. Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi Data Security in Cloud Computing using AES under HEROKU cloud:IEEE 2018

[3]. S. Lei, Wang Ze-wu, "Research and Design of Cryptography Cloud Framework," IEEE. 2018.

[4]. S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, Abuja, Nigeria, 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[5]. Pandey S., Purohit G.N., Munshi U.M. (2018) Data Security in Cloud-Based Applications. In: Munshi U., Verma N. (eds) Data Science Landscape. Studies in Big Data, vol 38. Springer, Singapore.

[6]. Sarojini, G. & A, VIJAYAKUMAR & Selvamani, K.. (2017). Trusted and Reputed Services Using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud. Procedia Computer Science. 92. 506-512. Mezzovico, Switzerland.

[7]. B. Bindu, K. Lovejeet & L. Pawan, "Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm", International Journal of Advanced Research in Computer Science 9(2), 2017.

[8]. C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", International Conference on Electrical, Computer and Communication Engineering, pp. 1-5, 2019.

[9]. N Jirwan, A Singh & S Vijay, "Review and Analysis of Cryptography Techniques", Inter. J.Sci. Engineer. Res. 4(3): 1-6, 2019

[10]. Y. Sharma, H. Gupta & S.K Khatri, "A Security Model for the Enhancement of Data Privacy in Cloud Computing", Amity International Conference on Artificial Intelligence pp.898-902. doi: 10.1109/AICAI.2019.8701398, 2019.