JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A REVIEW OF CLOUD COMPUTING TO USE OF CRYPTO GRAPHICAL TECHNIQUES TO SECURE THE DATA

By - Sarika Hemant Gadekar

Guide Name Dr. Arpana Bharani

Abdul Kalam University Indore

ABSTRACT- Cloud computing is now a day's becomes the most attracted phenomena to use for large scale organization or for individual who need various network services with least cost. Normally individual's information is stored on public Cloud which is available to everyone for access. This fundamental raises some issue opposite to flexible services provided by cloud providers, like Confidentiality, Integrity, Availability, Authorization and many more. Recently, Lots of options are available to protect the data and most preferable ways is to use encryption. Encryption only can't provide enough protection while considering lots of users' sensitive information.

KEYWORDS- Cloud computing, Encryption, Cryptography, Data Security.

INTRODUCTION

Cloud computing proposes new model for computing and the associated problems of its as compute, storage, software program. Cloud computing has many buyers like average people, academia, and enterprises with purposes and motivations various to move more than to the cloud. If perhaps cloud computer users are actually academia, the security as well as functionality of computing as well as the cloud service providers (CSPs) need to be effective. The majority of the enterprises possess lot of information and they search for a storage area of cloud setting to secure the information. Hence, protection plays a crucial role in protecting those very sensitive information. There are lots of CSPs that supply the security of information of the users.

In the procedure of offering security for information, the CSPs create an inclination to tamper or maybe misuse the very sensitive information without the previous information of the users. Thus, the users are pressured to conceal the originality of the information of theirs prior to storing directly into cloud storage. There are lots of

standard present cryptographic strategies which assist the drivers to encrypt the information prior to saving directly into cloud storage. Each day the need for these cryptographic methods increases tremendously. The objective of encryption is making information unintelligible to unauthorised customers & incredibly tough to decipher when attacked. Encryption is able to offer good security for information to provide very sensitive details probably the highest amount of protection.

CLOUD COMPUTING

The term cloud can also be considered as a metaphor for the internet. The usage of the term cloud can be recalled from its common depiction in network diagrams as an outline of the literal cloud in the sky. The diagram is used till now to represent the cloud. It depicts transportation of data from one end to the other end across carrier backbones. The cloud does not have any physical boundary restrictions and has made the world a smaller and interconnected entity. Cloud has paved the way for globalization of computing and sharing, where people from all over the world can communicate with each other.

CLOUD STORAGE

The rapid growth of the data and the need to keep it safe and for a sufficiently long time requires organizations to set up a separate team to manage the data. The management work leads to operations involving procedures to take care of the resources to store the data and safeguard the data itself. All these processes need to be done from the initial stage of data creation till it is destroyed. These management related issues surrounding the data consume time and manpower.

With cloud storage, there is an opportunity for the user to outsource the data through the internet to an offsite storage. The offsite storages are provided and maintained by a third party. The user can rent the storage space to store his data. Later on, the user can access the data or retrieve the data through internet. A model of cloud storage is represented in Figure 1. In Figure 1, consumer represents the cloud user, internet represents the network. The cloud service provider rents its storage space to the user. The term cloud provider and cloud storage denote the same and hence used interchangeably in this thesis.

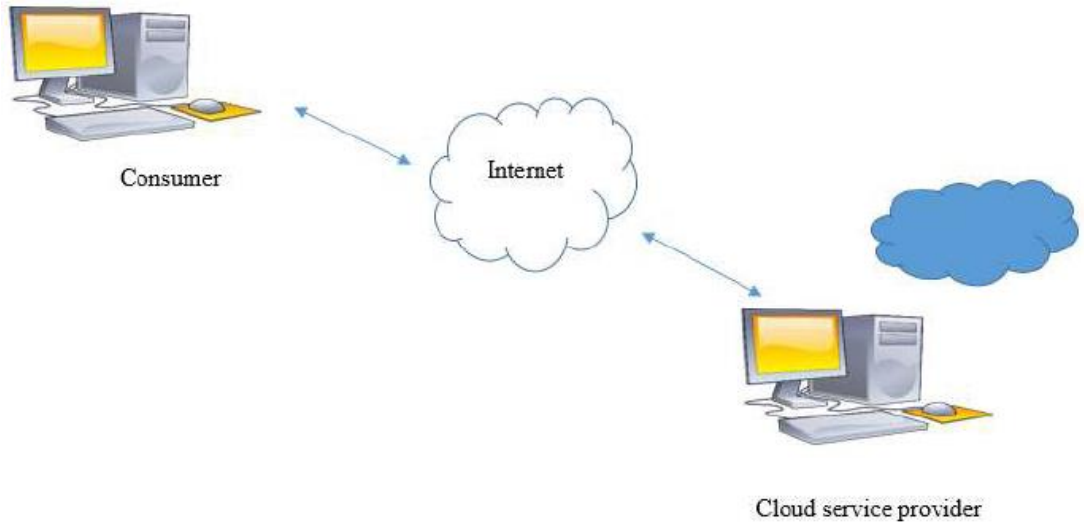

Figure 1: Cloud storage

Many businesses and enterprises use cloud computing, and cloud storage service because of their enormous benefits. But conducting business solely on the cloud leads to outsourcing some confidential files and sensitive data to a third party. In such an environment, the data are exposed to new risks.

The cloud provider which has the stored data may reside outside the user's premises. When the data goes out of a safe boundary, the safety rules or policies used to protect the sensitive data may go invalid. Hence, enterprises must take additional measures to secure the data in the cloud storage, beyond the basic protections offered by providers.

Some widely used cloud storages are listed below:

- Dropbox
- Google Drive
- One Drive
- Spider Oak

Most of these services are for free, but other providers charge the user based on per gigabyte data stored. As a number of providers have hit the market, the storage prices have started to drop. Out of all the benefits, the vital benefits of the cloud storage are listed below:

a) **Cost savings** – The infrastructure needed to store the data incurs a cost on the user side. This cost gets reduced when an external provider is used for storage.

b) **Accessibility** – The user can access his data wherever and whenever he wants. The access is not dependent on physical boundaries or time.

c) **Invisibility** – The place of storage is invisible to the user and hence some privacy can be maintained.

d) **Sharing** – Data is stored at a different location, and can be shared among multiple users.

e) **Disaster recovery** – The customer data is protected from any physical attack or hurricane that might happen at his place. Having the data stored on a off-site can be a help when the user wants to shut down or is being down for a few days or weeks. The benefits of cloud storage are enormous, but has some limitations or issues that make them less comfortable to be used. In cloud storage, data plays the primary role. But the data faces two main problems or issues as stated below:

f) **Data security** – The user data is stored in the cloud storage and it needs to be maintained in a secure manner.

g) **Data availability** – The user does not possess a local copy of the data and hence the data needs to be available to the user at all times

CLOUD DATA LIFECYCLE

As far as cloud storage is concerned, the user data is of the primary concern and plays a fundamental role. The life cycle of a data stored in the cloud storage is depicted in Figure 2. The data needs to be protected in each phase as stated below:

a) **Data creation:** The lifecycle of the data starts from the creation or storage of the data in the cloud provider. At times the same data gets stored in multiple cloud providers. The user data should not be stored in the raw format, but some transformations like encryption need to be done on it and stored.

b) **Data maintenance:** After the data are stored in the cloud provider, the data maintenance phase starts. No major operations are performed here, but the data needs to be stored safely before it is being downloaded by the user. The integrity of the data needs to be maintained.

c) **Data recovery:** This phase refers to the scenario, where the data can be recovered by the user if any of the cloud provider fails.

d) **Data deletion:** This is the final phase of the cloud data cycle, where the data are deleted in the cloud provider after its usage. The storage space occupied by that data is reclaimed by the cloud provider.

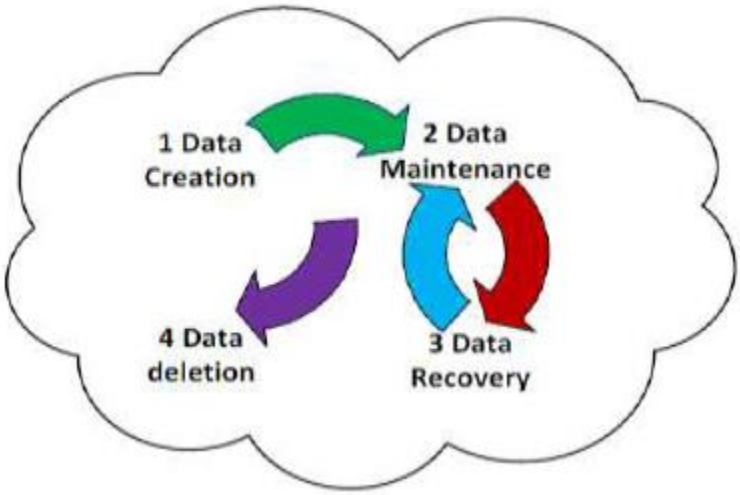

Figure 2: Cloud data life cycle

All these phases involve protection measures that need to be done by the user. The subsequent section discusses in detail the issues that pertain to the data.

Issues Pertaining to the Stored Data

The main issues that contribute to the safety of the data are discussed. The user's data should be confidential and even the cloud provider should not be able to view the data and this property is termed as confidentiality. The information on the cloud should not be modified by any entity other than the owner, termed as integrity. The service imparted by the provider should be available to the user at all times without any disruption, termed as availability. Accountability allows the members of a cloud system to ensure that obligations to protect data are observed by all users who process the data, irrespective of where that processing occurs. Privacy relates to the data privacy, which is the ability of an organization or an individual to decide about which data in a computer system can be shared and with whom. As stated, there a number of issues pertaining to the data stored at the cloud provider. This thesis aims to bring out solutions for the issues concerning data security and data availability. Both these issues are dealt in detail in the following section.

DATA SECURITY

The data stored in the cloud provider is vulnerable to a number of attacks by an inside entity or by an outside entity. Thus, the user data needs to be secured from these kinds of attacks. Protecting the data could be accomplished by any one of the three participating parties: third party, user, and Cloud Service Provider (CSP). The approach followed by the third party is to make use of a Third Party Auditor (TPA) to verify the integrity of the data at intervals of time. If the user is responsible for checking the integrity of the data, the user needs to take many precautionary steps to maintain the integrity of the data. Some of the steps that the user takes is to encrypt the data and store the encrypted data. The CSP or the server also takes some actions to verify the integrity of the data.

This paper looks at the security measure taken by the user to protect the data. Of all the different models developed, one of the widely used solutions is to make use of crypto graphical techniques to secure the data. The following section gives an overview about cryptography.

CRYPTOGRAPHY

Cryptography is a science of keeping the information secret. It is a method of storing and transmitting data in a particular form so that only those persons for whom it was intended can access the data.

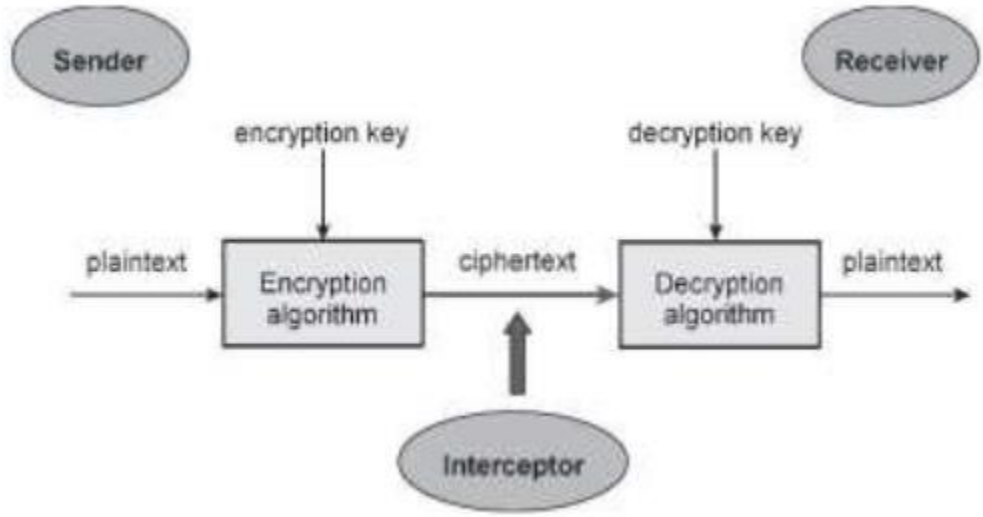

Figure 3: Cryptosystem

1) **Confidentiality** – Information should be accessible to users who are authorized to have it. It should not be accessible by those entities who do not have authority to do so. There are a number of techniques through which confidentiality can be implemented. These techniques range from physical protection to mathematical algorithms which render the data unintelligible.

2) **Data integrity** – should protect the information from unauthorized alteration. To enable integrity, the cryptosystem must have the ability to detect data manipulation by unauthorized users.

3) **Authentication** – the cryptosystem should allow access to the data based on the user identification. The user should authenticate himself before doing any operation on the data. If two users want to enter a communication, they should identify each other. The information that is delivered over a channel should also be authenticated based on the source of the data, the date on which it was sent, the data content and the time sent.

4) **Non-repudiation** – should give an assurance that an entity has sent a message or has signed a document. Repudiate is to deny and nonrepudiation is for an entity not to deny a message sent by him. The basic terminologies used in cryptography are:

1) **Plain text:** This is the original information or message that is of value and needs to be maintained in a secure manner. The plain text usually pertains to a particular user who may share it with someone or might use it only for himself.

2) **Encryption algorithm:** This is an algorithm that is used to secure the plain text. It converts the plain text into a different format which is done at the user side. The algorithm uses various substitution and transformation functions on the plain text.

3) **Secret key:** The secret key or the encryption key forms as an input to the encryption algorithm. The key is a value independent of the plain text. The encryption algorithm will produce different outputs depending on the key being used at the time. The exact substitutions and permutations performed by the algorithm may depend on the key

4) **Cipher text:** This is the encrypted message in a different format when compared to the plain text. The message will be in an unreadable form depending on the secret key and on the encryption algorithm. When the same plain text is submitted to the same encryption algorithm with two different keys, the output got from the two algorithms will be different. The cipher text is a random stream of data that is unintelligible.

5) **Decryption algorithm:** This algorithm is the inverse of the encryption algorithm. At times, the decryption algorithm will be the same as encryption algorithm in the reverse order or at times it may differ a little from the encryption algorithm. This algorithm takes the secret key and the cipher text as the input to produce the plain text.

TYPES OF CRYPTOSYSTEMS

There are two types of cryptosystems based on the manner in which encryption and decryption are carried out in the cryptosystem

- Symmetric key encryption
- Asymmetric key encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated and it is practically impossible to decrypt the cipher text with a key that is unrelated to the encryption key.

Private Key cryptosystems

Private Key cryptosystem, also termed as symmetric cryptosystem, is a form of cryptosystem in which the encryption and decryption are executed using the same key. It is also mentioned as conventional encryption by some authors. Private Key cryptosystems use substitution and/or transposition techniques. Substitution is a

process where each element in the plaintext is mapped into another element. Transposition is a procedure, whereby, the elements in the plaintext are rearranged. The private key cryptosystems usually consist of a set of encryption and decryption transformation functions {Ee Є k} and {Dd Є k} respectively, where Ee and Dd are the encryption / decryption functions and k is the secret key. The block diagram of a private key cryptosystem is given in Figure 4. There are a number of encryption algorithms that follow the private key cryptosystem like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Twofish, Serpent and much more. The most widely used algorithm was DES till 2000. But in 2001 the NIST published AES which replaced the DES algorithm (Daemen & Rijmen 2001).

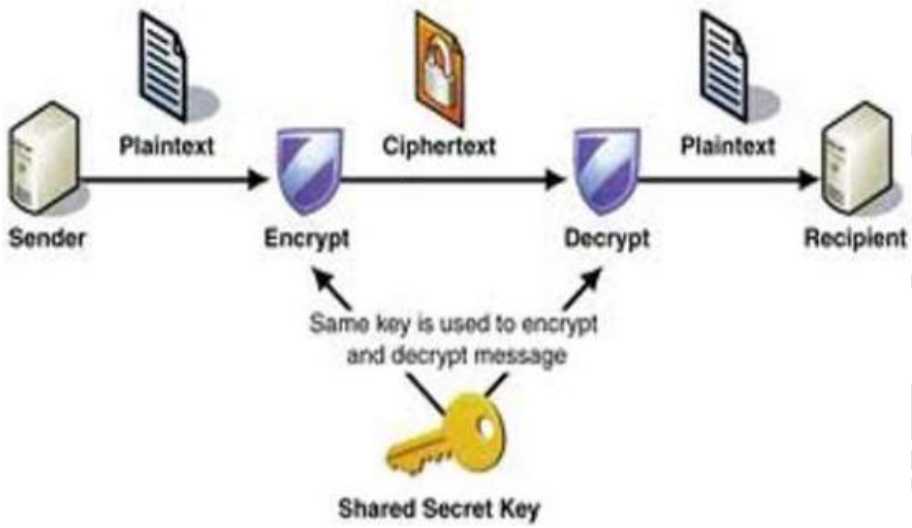

Figure 4: Private Key Cryptosystem

Public Key Cryptosystems

Public Key Cryptosystem also termed an asymmetric cryptosystem, is a form of cryptosystem in which encryption and decryption are execute during two different keys, a public key and a private key. The model of a public key cryptosystem is given in Figure 5. In public key cryptosystem, encryption transforms the plain text into cipher text using one of the two keys and an encryption algorithm. Using the other paired key and the decryption algorithm the plain text is retrieved back from the cipher text. Public key algorithms are based on mathematical functions. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication. Public key cryptosystem evolved from an attempt to attack the key distribution problem associated with private key cryptosystem. The next section discusses the data availability issue.

Figure 5: Public Key Cryptosystem

SIGNIFICANT BENEFITS OF CLOUD COMPUTING

- Adoption of cloud computing in organization increases the business flexibility
- It helps in cost reduction
- It solves the problem of automatic software or hardware IT solution upgrades
- It increases agility that is able to adapt quickly to respond the changes in a business environment.

CLOUD SECURITY AND PRIVACY VIA OBFUSCATION

The procedure for transforming a code semantically to the same form of it is actually termed as obfuscation. This particular procedure uses the code really harder to understand even if the source code can be purchased with the assailants. The reverse engineering is actually made harder with using obfuscation. The likely security threats in cloud computing earth is actually overcome making use of this possible obfuscation strategy [twenty four] by securing the APIs, the shared applications & infrastructures. This particular area offers a comprehensive survey on the presently existing obfuscation methods which covers the security overhead, limitations, security in resource sharing as well as performance efficiency improvements.

- **Data Obfuscation with Steganography** In order to improve the security of cloud storage, proposed an obfuscation as well as steganography method which assures confidentiality. At this point, the obfuscated information is embedded within the picture which tough the procedure of differentiating the cover picture as well as stego reputation. The enter information is obfuscated utilizing MRADO method and then the embedding is performed using LSB embedding method.

- **Data Obfuscation with Matrices** Likewise, an obfuscation method without utilizing encryption method is actually suggested which preserves the data privacy as well as confidentiality while in the lack of encryption to cloud servers. At this point, the dimension of matrices is actually resized without using false data. To do so, with regards to the dimensions of the matrices, each row as well as column are actually split in to a lot of splits which will keep the selection of matrices as it's.

- **Local Differential Privacy Obfuscation** Additionally, for IoT data analytics an obfuscation framework is actually recommended based on differential privacy as well as edge computing. At this point, the privacy is actually assured with Local Differential Privacy (LDP) data obfuscation. Each server utilizes LDP framework for saving the data and then forwards the distilled data to the cloud server.

- **Malware Obfuscation** Malware obfuscation methods are actually explored [thirty], which defeats antivirus scanners. This particular paper proposes the metamorphic and polymorphic malware based obfuscation method which contains Code integration, code transposition, instruction substitution, subroutine reordering, register reassignment, and Dead-code insertion. To alter the initial look of the data, the dead code insertion contributes virtual directions to a program

- **Code Obfuscation** For that reason, code obfuscation is actually proposed, which utilized a code obfuscation engine (CobE) to obfuscate applications by executing code stirring as well as safeguard the initial data. In code stirring, jump guidance are actually added to spot the execution path by relocating the little unique code chunks of the binary file. CobE is actually a hijacking protection mechanism which protects the user programs from reverse engineering attacks.

- **EncryScation (Encryption and Obfuscation)** An EncryScation strategy is proposed [thirty six], that is a unique strategy to secure data by using encryption at the prospect side in addition to obfuscation at the server side. The obfuscated information is saved on CSP(Cloud Service Provider) database which safely retailers both Data Owner/Data User(DO/DU) data and also shields from data tampering or perhaps misuse.

- **Code Transformations with Obfuscation** A comprehensive survey of obfuscation strategy is recommended that implements code obfuscation by 3 diverse sessions including layout transformation, control flow transformation as well as data obfuscation. The modification of the layout as formatting, comments removal, scrambling and identifiers is actually carried out in layout transformation. For control flow transformation, the system flow is altered the place that the computation function retains the same.

- **Programming Languages Obfuscation** Obfuscated programming for coding is actually suggested together with weird languages construction for coding. For literary code evaluation, the programming contexts as well as the literary contexts are actually joined utilizing obfuscation as well as weird

languages. In software development, the benefits of code reading by human are actually highlighted by weird languages as well as obfuscated code.

LITERATURE REVIEW

Hu, C., Liu, et al (2019) the writer centers around how you can construct a PEKS diagram by means of obscurity. The essential strategy is founded on the Differing Inputs Obfuscation (DIO) and also may be looked at as an underlying endeavor to use DIO in the PEKS discipline. With this paper, the writer centers around how you can create an open major encryption with catchphrase seek conspire (PEKS) by means of muddling. To the pleasure of ours, we discover that DIO could be used manufacturing PEKS programs. Using contrasting energy sources of information confusion in PEKS field and get a couple of intriguing hypothetical results. This particular paper exhibits a crucial PEKS plot supporting one-time catchphrase appearance which may be properly reached out to assist complicated functionalities as well as to that in the multi customer environment. We think about the KGA security of PEKS and enhance our important program to oppose disconnected watchword speculating assaults. Contrasted and PEKS plans opposing KGA assaults, this strategy is actually a regular one rather than a PEKS conspire with an assigned analyzer. The confinement of this strategy is actually self-evident, *i.e.,* the trapdoor produced procedure is actually wasteful which might cause them to become inapplicable in asset limited factors. Disdain of the results gotten by using muddling in PEKS development, it should be brought up that these PEKS plans fail to verify the accuracy as well as culmination of the query product from the server.

Akshay, K. C., & Muniyal, B. (2018) these days keeping and providing up the security as well as trustworthiness of the information while it's replaced via available routes is actually a serious undertaking. In order to overcome this test the writer will provide a technique to confirm the information via image steganography. It's an altered LSB image steganography technique which makes use of secret term to shroud the information in an image. For concealing the information a next strategy is followed to which great for nothing code are actually made as well as the coordinating is dependent on secret word coordinating. In this particular paper, 3 strategies are actually broke down to spare the great for nothing code: Method one, Method two, and Method three. In Method one, higher pinnacle flag to commotion proportion esteems that are acquired. In method two as well as three both have crest flag to commotion proportion esteems that are tantamount still the Method three is actually controlled and is dependent on the conditions in number of bits to store.

Bieniasz, J., & Szczypiorski, K. (2018) the writer considered applying 2 steganographic tips (socialsteghash as well as steghash) for another appropriated correspondence framework by satisfying presumption for cyberfog security strategy. An additional concept of the conveying framework realizing the chance of cyberfog security was shown the program consolidates and changes a few of segments, for instance, steghash for buying information. Socialstegdisc for trustMASS as well as filesystem pursuits for gadget to gadget information

transmission Security is actually portrayed by the manner in which that the halfway trading off of the framework doesn't interface the activities, while caught assessments are actually useless for the foe.

Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017) the writer centers around creating a protected cloud biological system wherein we use multifaceted verification alongside many different dimensions of encryption as well as hashing. Alongside the recreated results The calculation portrays the functioning of the framework by speaking to the entire process from client validation to recovery as well as capacity of client information from cloud. This particular paper exhibits a combination cryptography framework which joins the benefits of both lopsided and symmetric encryption. Protected cloud biological society is recommended guaranteeing information security as well as protection by actualizing several encryption methods at dimensions that are various. The framework also utilizes specific hashing and salting methods which perhaps quality the entire encryption procedure, similarly guarantee thought verification along these lines permitting the part of one time password, as well as would like to sign up straightforward developments which would increase the proficiency as well as simplification of the frameworks of ours.

Mumme, D. C., et al (2017) the writer portrays a multilayer security framework called "Application Protected Execution"(APEx) which has a " In VM observing" usefulness guaranteed by out-of-band mind made within a virtual machine on cloud based hubs. The paper also portrays an application which employes APEx to shield client room programming from finding out and return situated programming (ROP) assaults. The software "Code Obfuscation Engine" (CObe) perform code blending as well as employs framework gets and out-of-band mind to obscurity plan stream and return the stack. Utilizing APEx, it is able to hop into out-of-band remembering for execution of fragile code territories, figuring of bounce concentrates as well as return addresses. This guarantees applications stream against higher jacking particulary assistance flood as well as ROP assaults. CObe modifications a two-fold history for using with APEx secured execution legally and doesn't need source code. The results are extremely encouraging for the delivery angles for the self-obscurity apps. Notwithstanding for execution fundamental program with limited registered assets, you will find a great deal of things that may be used bringing about influence to execution. Notwithstanding for the outrageous situation incidental emplacement of MS administrators for hardening the obscurity must be feasible at important functions of the code for minor by and big effect. This particular paper concentrated on the program as well as execution of the out-of-band GSIM level as well as the code obscurity, code mixing, and code concealing using the GSIM level.

CONCLUSION

Cloud computing provides numerous advantages to user but still due to security issues many users hesitate to adopt it as well the service provider may have a issue about un authorized access. So, to solve issue related to both user and service provider, we developed a new framework by proposing combination of encryption and obfuscation technique together. Before sending data on Cloud encryption, it provides security to the data which

is on transition in the network by which user ensures the confidentiality of his data. Many techniques towards solving the issues of data privacy and security are depending on cryptographic encryption and decryption methods.

REFERENCES

[1]. Hu, C., Liu, P., Yang, R., & Xu, Y. (2019). Public-Key Encryption With Keyword Search via Obfuscation. IEEE Access, 7, 37394- 37405, 2019

[2]. Akshay, K. C., & Muniyal, B.. Analysis of Data Hiding Methods in Image Steganography. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2023-2027). 2018

[3]. Bieniasz, J., & Szczypiorski, K.. Towards Empowering Cyber Attack Resiliency Using Steganography. In 2018 4th International Conference on Frontiers of Signal Processing (ICFSP) (pp. 24-28). IEEE, 2018

[4]. Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 288-292). IEEE, 2017

[5]. Mumme, D. C., Wallace, B., & McGraw, R. Cloud Security via Virtualized Out-of-Band Execution and Obfuscation. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 286-293). IEEE, 2017

[6]. El Makkaoui, K., Ezzati, A., Beni-Hssane, A., & Motamed, C. Cloud security and privacy model for providing secure cloud services. In 2016 2nd international conference on cloud computing technologies and applications (CloudTech) (pp. 81-86). IEEE, 2016

[7]. Handa, K. and Singh, U., 2015. Data security in cloud computing using encryption and steganography. International Journal of Computer Science and Mobile Computing, 4(5), pp.786-791, 2015

[8]. Zhu, Z. and Jiang, A secure anti-collusion data sharing scheme for dynamic groups in the cloud. IEEE Transactions on parallel and distributed systems, 27(1), pp.40-50, R., 2015

[9]. Xiao, Z. and Xiao, Y., Security and privacy in cloud computing. IEEE communications surveys & tutorials, 15(2), pp.843-859, 2012.

[10]. Parah, Shabir A., Javaid A. Sheikh, and G. M. Bhat. "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique." In 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET), pp. 192-197. IEEE, 2012.

[11]. Raj, Y. S., Rabara, S. A., & Kumar, S. B. R. (2022, January). A Security Architecture for Cloud Data Using Hybrid Security Scheme. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1766-1774). IEEE.

[12]. Kapoor, J., & Thakur, D. (2022). Analysis of Symmetric and Asymmetric Key Algorithms. In *ICT Analysis and Applications* (pp. 133-143). Springer, Singapore.

[13]. Sabeti, V., Sobhani, M., & Hasheminejad, S. M. H. (2022). An adaptive image steganography method based on integer wavelet transform using genetic algorithm. *Computers & Electrical Engineering*, *99*, 107809.