VOL. 14, NO. 7, APRIL 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DATA SECURITY IN CLOUD STORAGE USING ADVANCED ENCRYPTION STANDARD AND HONEY CRYPTOGRAPHY

S. Arun[1] and N. R. Shanker[2]
[1]Ponnaiyah Ramajayam Institute of Science and Technology University, Thanjavur, Tamil Nadu, India
[2]Aalim Muhammed Salegh College of Engineering, Chennai, India
E-Mail: ksarunsampath@gmail.com

ABSTRACT

In Cloud computing, data security has an important role in the communication system development. Network security has become a major concern in the recent years because, in cloud storage environment, the data should be secured from the intruders. So the data should be encrypted and outsourced in the cloud. Cryptography serves an important role in the information security system against different attacks and cloud storage systems. New types of cryptography techniques can overcome the security threat. The Advanced Encryption Standard is a robust symmetric key cryptographic algorithm that uses the lookup table to enhance its performance. The Cache Timing Attack relates the encryption timing details under a key already known with a key that is unknown to infer the key that is unknown. Here an extension of a public-key cryptosystem is proposed which is a combination of Advanced Encryption Standard and Honey Cryptography to support a private key cryptosystem. The results have been obtained by Advanced Encryption Standard key length as 128 bit and no. of iterations as 10.To improve competency and to reduce drawbacks, this paper proposes a honey encryption scheme. The parameters to be discussed focuses on the no. of iterations, key length, and the side channel attack type to be implemented.

Keywords: cloud computing, symmetric key cryptography algorithm, data security, advanced encryption standard and honey cryptography.

INTRODUCTION

The concept and techniques for implementation of cloud computing is widely resourced all over the world. The theoretical knowledge about the cloud computing confused the actual representation of cloud computing. Several firms and enterprises provide services in the name of cloud computing which are originates from the network topology. The traditional cloud framework is shown in Figure-1. Cloud computing represents the services or applications provided through an internet. [1] Cloud-based systems are not emerged rapidly; the development of the cloud system was traced from the conventional systems in which the resources and applications are remotely shared with client and servers.

The varieties of different services and applications are fetched through the clouds. Applications and devices are used in the numerous cases, it involve these services not extraordinary function. These services available in many companies, its get from the cloud. It has produced the following services from cloud computing: online service, share point, it permits the business intelligence tools and contents are uploaded to the cloud such as it makes office applications useable in the cloud.

The google cloud storage providing a lot of services for large infrastructure, I T companies, and the former users. [2] For the customers, salesforce.com it makes the own cloud services. [3] Further other paid services and Vmforce, are grown up services in nowadays. [4] Anywhere, this cloud clue is not clear, and the question is why the cloud computing happen, and whose care about the cloud platform, and how about the encryption and security. These sections are providing a knowledge about deployment models, cryptography features, advantages, service models Z, characteristics, along with cloud computing.

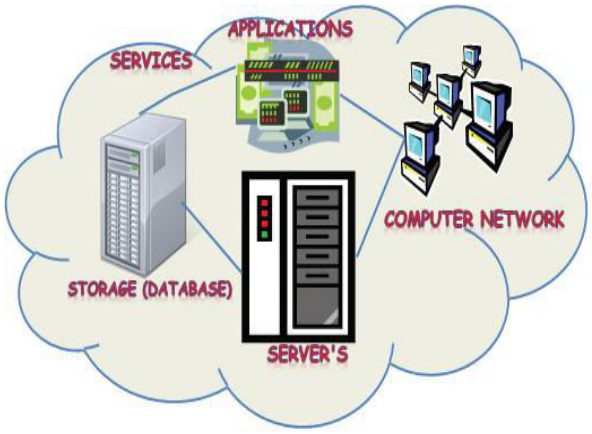

Figure-1. Cloud computing.

CLOUD COMPUTING FEATURES

Cloud computing has the following various features are:

a) Distributed infrastructure: Cloud computing is a software virtualized frame work, and the examples are physical services optionally shared and networking capabilities. Cloud computing could be used for storage. The deployment model cloud infrastructure is built up visible infrastructure to the user identification number.

b) Dynamic provisioning: Automatically permitted the services for literal necessity by using software automation. From the service capacity, compression and elaboration are optional, and this dynamic scaling is targeted, when maintaining the protection and high reliability.

c) Network access: To attain an across the board accession to mobile devices, laptops, and PCs, an internet

connection is a need, it is through on standard API representatives based on HTTP. This deployment by using the cloud services and include the business practical applications into cutting-edge applications in the current smart phones.

d) Managed metering: The meter for optimizing and managing service and for billing data and supplying reporting is used in this cloud computing. It provides the scalable services, and multiple sharing is required through any location. For this service, actual usage based on the consumer is charged.

SERVICE MODELS

When the cloud computing was created first, the services offered was deployed in business conditions along with high demands as shown in Figure-2. The following examples are:

Software as a Service (SAS): Consumers are buying the ability to access and then use an application based on services in the cloud hosted.[5] Increasing the Microsoft involvement in this side, as well as Microsoft Office 2010 is the part of the cloud computing. Its Web Apps are approachable to licensing customer's office volume and Web App office subscribers by the cloud based on online services.

Platform as Service (PaS): Consumers are purchase accession to platforms to deploy their applications and own software to the cloud. [6] Consumers do not control the network access and operating systems, and it contains only where can be deployed their applications.

Infrastructure as Service (IaS): Storage, Consumers control, system management processes, network connectivity it does not preserve the cloud infrastructure. [7] In a market or an industry different subsets of cloud models are recognized. Communications as Service (CaS): This is one of the subsets models its used to differentiate IP hosted telephonic services. This CaS is a shift into additional numerous Session Initiation Protocol (SIP) and IP communication centres. [8] In this cloud SIP facilitates and installing IP is the Private Branch Exchange. [9] CaS is considered a subset of SaS preparation models.

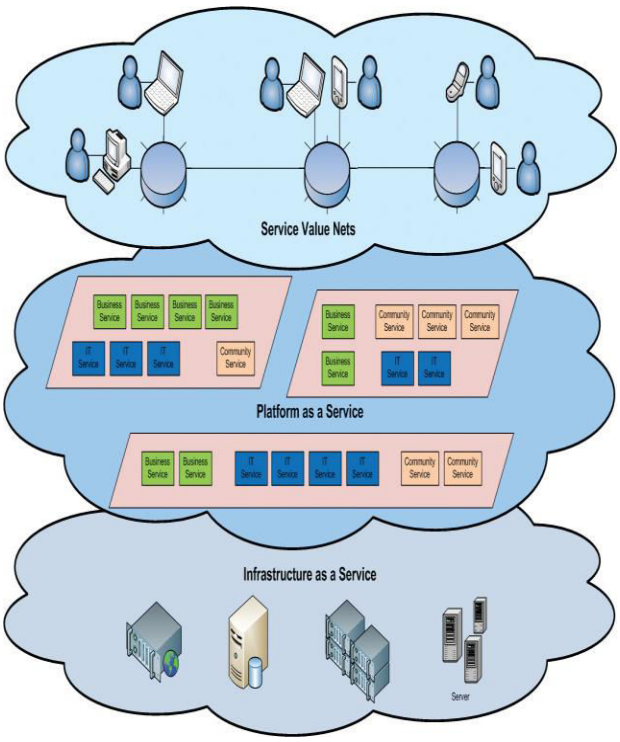

Figure-2. Service mode.

CLOUD DEPLOYMENT MODELS

Cloud computing is the required problems. These four models are deployment that could be followed to address the problems is as follows:

a) Private cloud: is the deployed, engaged, and observed, for a peculiar distance area. It would be through the internet connection, such as from the branch-branch.

b) Public cloud: This substructure is required for the users if an example is Google-Drive services. In fact, public clouds have enabled a consumer to improve and spread service in this cloud along with a little fiscal outlay and its combined with the capital generally required, and other cloud computing services available.

c) Hybrid cloud: Whatever the cloud infrastructures have numerous clouds in several areas. Clouds are allowed only the data or peculiar data that can be permitted shifting between the clouds. Public and Private cloud be combined and to support the organizational information and offer services through the cloud.

d) Community cloud: This cloud is applied for the large infrastructure, as well as government organizations that related to the single cloud to upload information with unified data or a server campus that associate with the single cloud computing community.

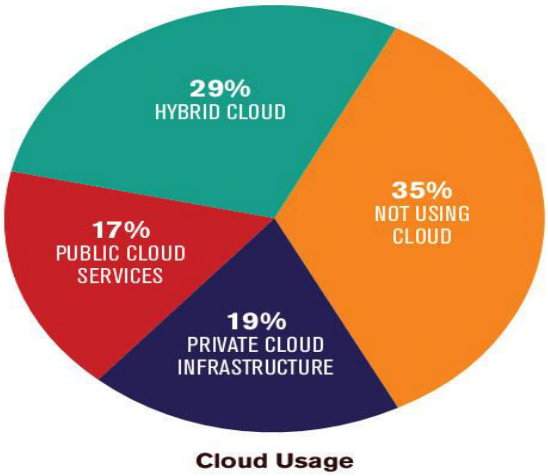

Figure-3. Cloud Computing Usage.

Enhancing attention is to the cloud computing attacks as discoursed above. This attacks are may be done with the various purposes, as well as for deriving valuable information on prominent scale organizations or forging personnel data. Figure-4 shows that how an attacker can inter penetrate with a virtual machine to the hypervisor of these cloud surroundings

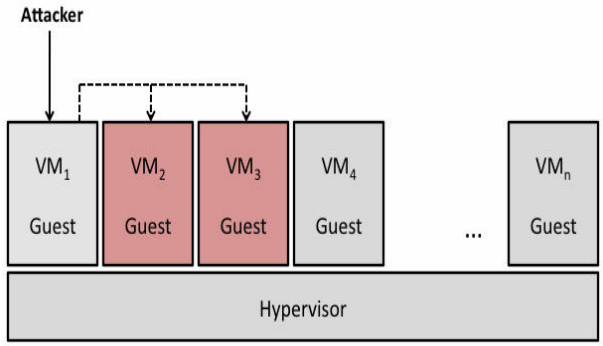

Figure-4. An example of attacking case to virtual machine.

Cryptography involves changes of clear text to an unreadable form. In this Cryptographic technique is used to change the contents safely by assuring that can read only the intended recipient. This spotlight domain can give an overview of cryptography of the history, and most of the complex, and the imaginative methods are used in enterprise contemporary encryption.

Cloud Computing Encryption

For cloud computing, the Encryption world is crucial problems that need to look into the various studies. In our cloud computing, the Encryption is identified based on the encryption. As encryption examples follow:

Encryption: E_1 and $E_2$are the two entities of cloud computing. The Entity identity is E2 is $ID_{E1} = DN_0 \backslash\backslash DN_1 \backslash\backslash DN_2$. The encrypt message M with ID_{E2}, E_1 as follows:

1.Calculate

$P_1 = H_1 (DN_0\ DN_1)$

$P=H\ (DN_0\ DN_1\ DN_2)$

2. Choose a random $r \in \mathbb{Z}_q^*$;

3. Output of the ciphertext

$$C = < rP, rP_1, rP_2, H_2(g^r) \oplus m >$$

Where $g=e(Q_0\ P_0)$ can be computed.

LITERATURE SURVEY

In cloud computing Data privacy is a basic problem today, as well as homomorphic encryption systems, are recommended for the data security. In fact, the sensible data could be maintained even, the cloud server behind this fully encryption homomorphic systems are permits the encrypted processing data that no need of prior decryption. Here homomorphic full encryption system from integers is presented. [1] For the secure processing data applications are, the operating encrypted data makes that Fully Homomorphic Encryption (FHE) Grain Holy. An (FHE) has not attained through symmetric cryptography; this application only needs secret keys. [2] Our encryption system could be used to secure a sensible data in cloud computing. This system is applying for one key and maximum ring integer as clear space text. For example a symmetric encryption system. [1]

The bootstrapping and public key needs essentially to refresh the noisy ciphertexts. An advanced method to make the homomorphic system, but the fully homomorphic its not requiring bootstrapping. Our system applies symmetric keys & have superior performance to being public key systems. [2]

In the storage distributed the vital idea is remote data uprightness. It gives the documents of the client and outsources client, without download the entire data. The client needs few circumstances for records to be numerous continued cloud servers, to provide cloud servers better expectation and security. The identity based distributed provable data possession (ID-DPDP), for assuring remote data in various cloud servers. This advanced model could be given various levels of checks. The Elliptic Curve Cryptography) (ECC) evaluation is used for encryption symmetric algorithm and producing keys for the data encryption & the undermined idea records are presented here. In our model additionally to increase the framework security utilization, it is employing the select cloud service provider (SelCSP). [3]

Cloud computing is a centralized and distributed network of inter related and inter connected systems with more than one IT sources based pay on demand usage. Even though users or cloud consumers are most flexible with the cloud resources. Is that main is security issues. [4] In nowadays Data security is the main problems, especially for the internet usage. Cloud computing requires speed, secure, and cryptographic area efficient techniques. [5] Privacy and Data Security, access management and identity, Business planning continuity / Disaster Recovery etc. and crisis concerned to data stored in the cloud. The cloud users are related to that data, but the security is the major issues dealt with seriously. The user's security data can be attained through the cryptography conventional method. Encryption is

completed through the asymmetric or symmetric key algorithms as well as DES, AES, RSA, Triple and Blowfish DES, etc., RSA algorithm, where the asymmetric key algorithm is employing two various keys for decryption and encryption process. [4]

Cryptosystem Blowfish is a fast and strong algorithm, applied to the cryptography. This RSA algorithm generally conceived for digital signatures. This method presented for a hybrid Cryptosystem is applying the Blowfish algorithm and RSA. A hybrid cryptosystem is conceived for a cloud computing, while the digital signature is shall for authentication user. So that this method gives features of both asymmetric and symmetric cryptography [5] this advanced method to minimize the decryption and encryption process through separating the file to blocks and increases the algorithm strength through enhances the key size. [4]

Cloud paradigm computing is used because of the low up & front price. Nowadays mobile phone users also store the data in the cloud. Customer data stored at the cloud and it requires to be saved the service provider cloud as well as potential intruders. In transit & data, threat into the data, at the cloud because of various possible attacks. Organizations are reassigning the crucial information to a cloud that enhanced all over data security. The cryptography is a general method to save the sensitive data in the cloud. Cryptography needs to manage the decryption and encryption keys. [6]

In this method, a new effective homomorphic encryption system based Lucas theorem is presented. [7] Homomorphic encryption probably secures encryption asymmetric solution to the problem, anywhere it computation cost and high storage. (8) In our cryptosystem permits various AND gates all over cloud encrypted data. The price of the two ciphertexts one AND is equal to the price of enhance on numbers. This advances method applies the {0, 1} as one key and cleartext space for decryption and encryption system. A homomorphic encryption system is a powerful tool that permits the performing computations it is no need prior decryption. [7]. in cloud computing, the encrypted processing data is an effective solution. Earlier encrypting data storing in a remote cloud server is highly urged, merely while using symmetric traditional algorithms as 3DES, AES. [7]

This advanced method is used on two computing tasks, dot product and Euclide squared distance. Random Projection (RP) and Compressed Sensing (CS) are lighter, but the lack privacy when the start with encryption uses the symmetric key is a projection random matrix. Sensing compressed encryption, multi-key is introduced in this method, and it calculates the basic general performance. The computing architecture comprises a Cloud, a User, & Trusted Third Party, it for disseminating the random CS keys. This TTP is having two learning machine modules, ML1 & ML2. The ML1 is applied to the cloud, ML2 applied to decrypts and the user side. This method is cheaper than encryption homomorphic regarding encryption time, data expansion, as well as storage, also used in multi-keys. [8]

Predicate-based encryption is a new cryptographic technique that gives fine-grained access control to encrypted data. Mostly it is utilized in secure cloud storage and biometric matching. Here a variant of symmetric predicate encryption is proposed that provide privacy preserving search operations that are controllable with un-decryptable delegated search and revocable delegated search [9].

Biometric authentication has become popular in large-scale industries. It requires an enormous amount of secure storage where the details of the registered user can be stored. High investment and maintenance cost is required for maintaining centralized data centres to store the information. As there is no guarantee for the cloud security, the user requires additional security. A new cloud-based biometric authentication system is developed using Microsoft cognitive face API. It is predominant to incorporate a security technique that can handle scalability. For single enterprise application over a full enterprise application, any user can utilize this system. Here the identification number that is text message related with every biometric image is protected by AES algorithm. For wider accessibility, the advanced method also operates under a distributed system [10].

The cloud computing environment allows users in the cloud to outsource their data into the cloud environment because of the ease of management and its cost efficiency. However, cloud users forget their control over the outsourced data to the cloud. This phenomenon becomes more vulnerable when initiating the handoff process. The issue occurs when the users in the cloud break some of the data access rights. The symmetric key encryption method eliminates this problem. However, this symmetric key encryption is not safe because a rejected user from the cloud gets backs to the system to acquire the secured data of mobile handoff devices. So a secure and efficient data sharing framework has been developed with proxy re-encryption and homomorphic encryption methods that prevent mobile cloud user's data leakage when the handoff process is initiated [11].

Mobile cloud computing has been emerged as a key enabling technology to eliminate the mobile devices physical limitations toward flexible and scalable mobile services. In the mobile cloud environment, searchable encryption is a key technique to keep usability and privacy of secured data outsourced in the cloud.To resolve the issue, several research efforts address the searchable symmetric key encryption and searchable public key encryption. Here a practical searchable encryption technique that supports updating operations in the applications of mobile cloud. A Personalized Search scheme over encrypted data is proposed with secure and efficient updates in the cloud [12].

Cloud is a business-oriented technology sharing data or information with excellent infrastructures. Cloud security is the subdomain of information security and cloud security. Here the cloud is used as a many service model and deployment model. There are different ways to monitor and secure the data and information from hacking. The suspicious activity for the customer data is through

data enhancing with encryption and decryption. Encryption forms the access method of justifying the original data to be duplicated form, and with proper decryption of the data, the client can be constructed to prevent the information from listeners from secret key encryption or symmetric key encryption. Before transmission between entities, the key should be distributed. In asymmetric key or public key encryption, the private and public keys are used in encryption level on the cloud. The public key is for encryption the file, and the private key is for decrypting the file [13].

Cloud computing becomes more popular in the computer field due to its ability in remotely storing and accessing data. It is mandatory to protect the data in cloud storage and access since the data transportation is through the public network. Here mobile cloud infrastructure is used for storing and accessing data. Thus an efficient cloud network is needed. A security framework for mobile cloud environment is needed that assures better data storage in an encrypted form in mobile devices and storage devices. A new security framework for data storage with Advanced Encryption standard is proposed [14].

Cloud computing gives the facility for enormous volume data storage and. It has a large capacity for storing individual data and many users simultaneously and provides the ability for its recovery at any time. Although cloud attracts many users, there is a unique requirement of security concerns. Here, a new security model is proposed that use the hybrid encryption and decryption concepts to give a protected and secure environment for data storage in the cloud. In the advanced model, the encrypted data is outsourced by the data owner at cloud server to hide from the intruder and only authorized user with decryption key can retrieve the data. The concept of symmetric key cryptography is utilized during encryption or decryption [15].

METHODOLOGY

Honey encryption algorithm is developed by Thomas Ristenpart and Ari Jules in the University of Wisconsin. The honey encryption provides more security over Brute force attack. The honey encryption provides a fake plain text when the chipper text is decrypted using an incorrect key. The attacker can get confused with the false data generated due to a false key and make him believe that the generated data is a legal data transferred in the network.

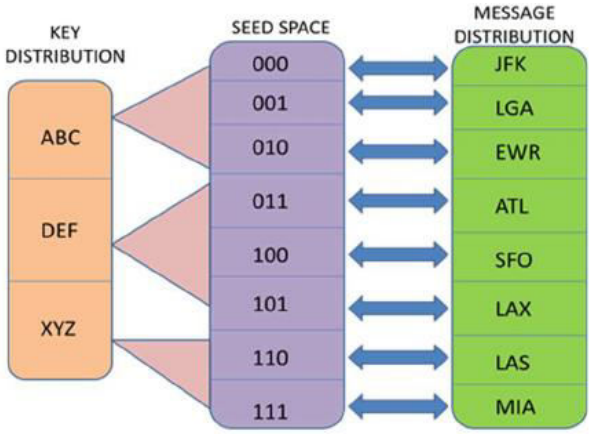

Figure-5. Distribution Transforming Encoder.

A message storage space, M is required to store all the possible data to be encrypted using honey encryption algorithm. Each data stored in the message space was linked with the seed storage space, s by the distribution transforming Encoder (DTE). The seed spaces act as a bit strings with length n. DTE acts as a linking function F for the seed space block to the message block. Figure-5 represents the flow of DTE in the honey encryption algorithm.

The perfect Distribution Transforming Encoder provides a perfect match between the seed space and message blocks. The seed space is randomly selected by the DTE to frame Data distribution. That means the function F of DTE is reversible. We can find the corresponding seeds based on the picked data bit. Function G is used to map the key distribution to the seed space using the honey encryption. The function G relates the keys with the seed space in a random fashion similar to that of Hash function. Based on the figure 5 the keyword ABC is connected to the seed space of 000, 001 and 010.

Thus, to encrypt the message M using the password k, we should figure out the seed space representing the message of function F which may be inversed.

$$S_m = F^{-1}(m)$$

Once the seed space is framed for the message block, then password related to the seed block is computed.

$$S_k = G(K)$$

After selecting the seed space and appropriate pass word then the encryption can be performed by XOR the Seeds measured above.

$$C = S_k XOR S_m$$

To understand the generation of chipper text an example of airport codes was illustrated in Figure-5. The message space, M represents the airport codes. M = {JFK,

LGA, ….., MIA}. The size of seed space is selected as 3 bits. The data bit ATL is selected as a message block with the password key as "XYZ". Applying the DTE the seed space for the selected data "ATL" is mapped as 011 and the seed space for the password key "XYZ" is 110. After generating the seed value for message and password, the DTE performs XOR on them which generates 101 as the encrypted chipper text.

$G(K)XORF^{-1}(m) = S_k XORS_m$
=011 XOR 110
= 101 = C

To perform decryption over the chipper text, DTE selects the seed value for the given password "XYZ" to regenerate the seed value 110. After generating the seed value, DTE XOR the seed value with the chipper text, 101. The original seed value 011 is extracted from it. DTE collects the decrypted seed values and maps the exact data from the message distribution. The airport code "ATL" is decrypted from the chipper text.

If the chipper text is processed with the wrong password. The process will result in the generation of believable fake results. Taking the same example and decrypt with the wrong keyword "DEF". The seed value for "DEF" is 011 and the seed value is XOR with the chipper text to get absolute seed value as 110. DTE maps the seed value and generates the airport code as "LAS". Thus, the generated message is also a valid airport code, but it is not the transmitted code. The decryption using any possible password will generate the valid message. This property of honey encryption makes the hacker to believe the wrong message as the original one.

The Honey encryption can be used to encrypt the data's stored in the cloud architecture. To implement in the cloud architecture a new method namely Secure Repository Manager (SRM) is introduced. SRM helps the cloud architecture to store the data securely. The functioning of SRM is to divide the data into several pieces and the store the pieces randomly in the cloud server. The size of each data piece relates to the level of security applied to the data. The reduce in the size of the data pieces provides maximum sensitivity and critical data. The data pieces with medium size provides less sensitivity and critical. The bigger sized pieces are not sensitive and critical.

After completing the encryption of the message packet, the chipper text was divided into smaller chunks and stored randomly in the cloud memory. The location of chunks in the cloud server was maintained in Secure Repository Manager (SRM). To download the data from the cloud server, the SRM requires the details like location information, chunk size and password for decryption from the client side. Once the valid information is provided with the chunk files in correct order was generated by the SRM. Then the chipper text is processed using decryption methodology and the original data is retrieved back. HTTPS and SSH protocols are used to transfer the data from the cloud server to the client system without any damage in the transferred data. If any damage is detected in the stored data cloud server request the user to retransmit the original data.

Secure Repository Manager Database (SRM DB):

The SRM holds the information like File name, ID, server path during uploading, password keys and file pieces. The information is stored in the portrayed form in SRM DB. Figure 6 represents the SRM DB.

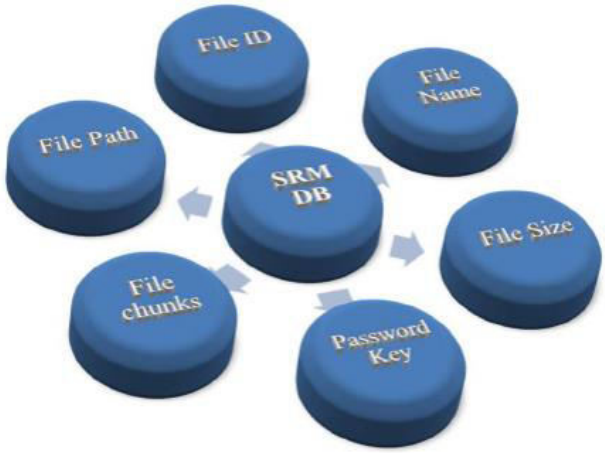

Figure-6. SRM Database.

The Data is encrypted before uploading the file to the cloud server and the decryption was performed after downloaded to the authorised user. The user is validated for authentication before downloading the data chunks. The authorised user holds the perfect key to decrypt the data to the original message. The file uploading and downloading algorithm are discussed below.

File Upload (Encryption):

- The cloud user transmits access request message to the SRM for authentication purpose.
- If Authentication success

Then SRM generates secure connection using HTTPS between User and Cloud server.
Else Request cancelled:

- The secured connection is established then the selected file is started to upload.
- At the initial stage of uploading the user was prompted with authentication password.
- Using the entered password, the honey encryption is applied over the data.
- Finishing the encryption process the data is chopped into several smaller chunks.
- The smaller chunks are then uploaded to the cloud server.

- Connection terminated after completing the upload operation.

File Downloading (Decryption):

- An access request message was passed by the user for Authentication form SRM.
- After the successful authentication SRM generates secured connection using HTTPS protocol between the cloud server and the client.
- The Data chunk was collected and downloaded as a package to the client.
- The user enters the password foe decryption.
- The password along with the packet size and location information is collected by the SRM.
- Decryption is performed the information collected by SRM helps the decryption function to maintain the original file structure.
- After successful decryption, the data was downloaded to the user system.
- Connection terminated after finish download.

Figure-7 shows the file access procedure between the user and the cloud server.

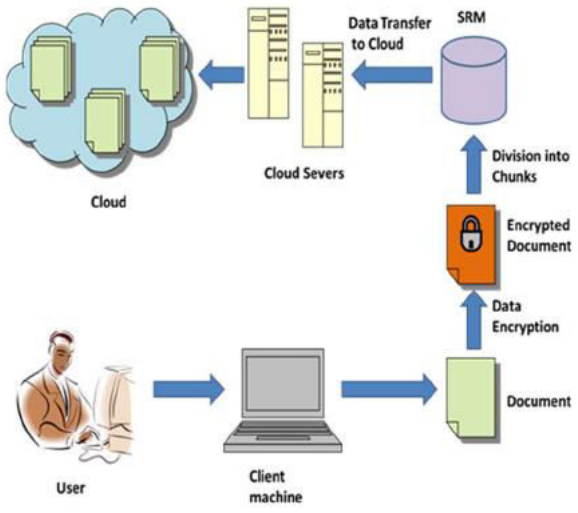

Figure-7. File handling from the cloud.

RESULTS AND DISCUSSIONS

The Honey encryption algorithm is implemented in the Network Simulator 2 platform, and the performance metric for the implemented algorithm is measured and plotted as a graph. Table-1 represents the parameters applied to the NS2 simulator to design the network using honey encryption.

Table-1. Parameters of the network.

Propagation	Two Ray Ground
MAC Type	802.11
Queue Type	Drop Tail/Print Queue
Antenna Type	Omni Antenna
Queue Length	500
No of nodes	50
Routing Protocol	DSDV
Plotting Area	1000*1000
Simulation Time	16s
Packet Size	100 bytes
Interval	0.05s

The performance metrics collected for the honey encryption is compared with DH keying and the blowfish algorithm.

Figure-8 shows the throughput plot. The throughput represents the amount of bandwidth consumed by the network or maximum transmission speed achieved by the network. The throughput is affected based on the delay, processing time and amount data retransmitted in the network. The throughput of the network determines the performance of the network. If the throughput goes low the performance of the network is also false down. So that the throughput of the system should be higher compared to the conventional methods. The network implemented with the honey encryption generates the maximum through put of 361kb/s.

End to end delay is the measure of time taken to transfer the data packet to the destination node in a unidirectional fashion. The end to end delay is determined by the packet loss ratio and the distance between the sender node and the transmitter node. The delay generated will affect the performance of the system by reducing the throughput of the network.

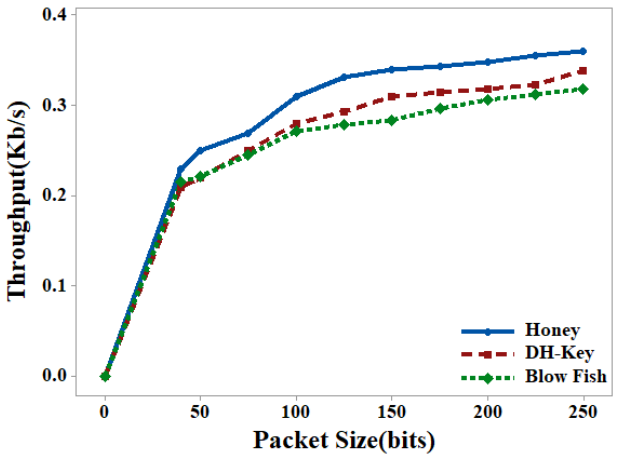

Figure-8. Throughput.

Figure-9 shows the end to end delay plot were the honey encryption generates the lowest delay value of 3.1ms which is 10 per cent lesser than the convolutional algorithms. The lesser complexity in encryption and decryption algorithm reduces the time taken for processing and transmitting the data in the network.

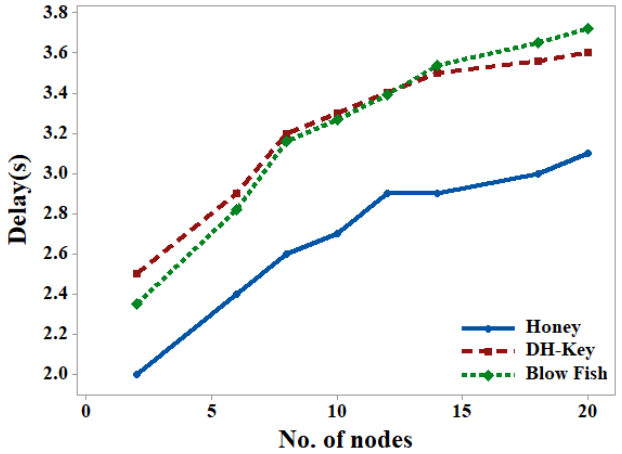

Figure-9. End to end delay.

Packet delivery ratio is the measure of the amount of successful data transmission between the sender and the user. The retransmitted packets are not measured in this plot. This measure is the inverse of the packet loss ratio. The packet loss ratio is the number of packets dropped during the transmission of data packets between sender and receiver nodes. The retransmitted data are measured individually which will not affect the packet loss and packet delivery ratio. The delay is measured considering the packet delivery ratio, packet loss ratio and the retransmitted packets. The Figures 10 and 11 shows the packet delivery ratio and the packet loss ratio of the network.

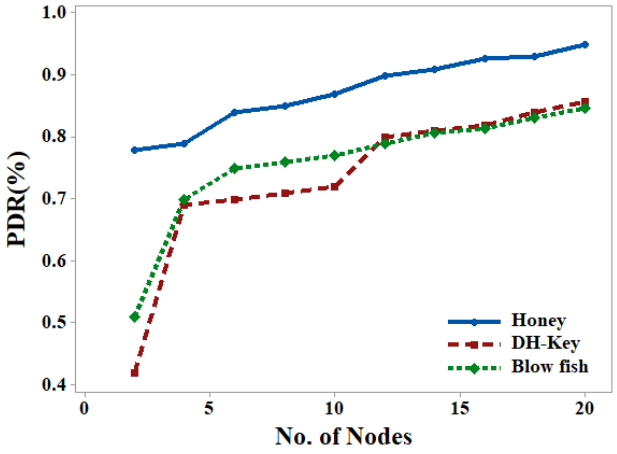

Figure-10. Packet delivery ratio.

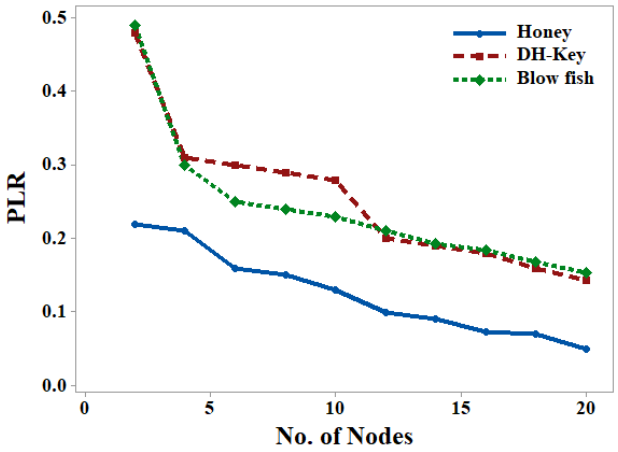

Figure-11. Packet Loss Ratio.

The Figure-10 shows the maximum Packet Delivery ratio for honey encryption is generated as 95percent and from the Figure-11 the packet loss ratio was achieved about 0.23 per cent and the remaining packets were retransmitted in further attempts.

The transmission and retransmission consume much power than the power consumed by processing of algorithm in the network. So packet loss an retransmission rate must keep low, and the packet delivery ratio should maintain high which improves the throughput of the network. The residual energy is the measure of amount of energy consumed by the network during the simulated time. Figure-12 shows the residual energy of the network.

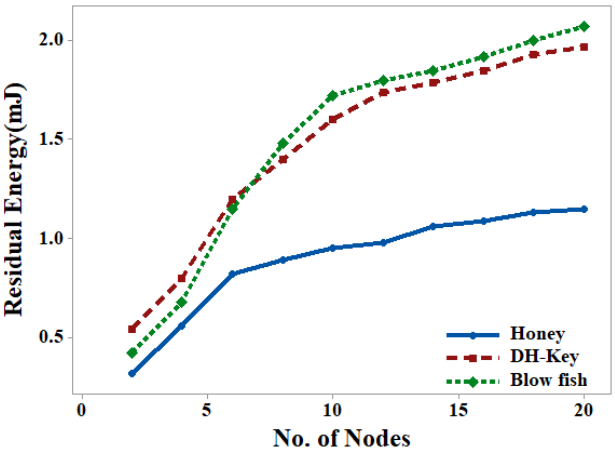

Figure-12. Residual Energy.

The initial energy of about 1000 joules is applied to the network, and Figure-12 shows the consumption of energy by different cryptographic algorithms.

CONCLUSIONS

Privacy and security of data is the primary concern in cloud computing data storage. Even though the cloud provides effective and readily accessible data storage and management, there are options for the intruder's presence and malicious activity. Data stored at cloud server is confidential and needs consideration.

Cryptography techniques provide a secure path for confidential data storage by using an encrypted form and providing its corresponding key to only authorize users. This paper proposed a hybrid symmetric encryption/decryption algorithm for secure data storage at cloud server. The key utilized for decryption process is shared to the specific user only. By utilizing the hybrid symmetric encryption honey algorithm is justified that it gives additional security for its data and user is assured that data retrieved is intact with no access of intruders. Since Cloud Storage Provider is the un-believed third party so can't store its confidential data in the crude form. Utilization of symmetric encryption makes the data effective against single encryption and makes it troublesome for the attacker to get the real data.

REFERENCES

[1] El-yahyaoui. 2018. Data Privacy in Cloud Computing. 2018 4th Int. Conf. Comput. Technol. Appl. pp. 25-28.

[2] S. Nitesh Aggarwall, Dr CP Gupta2. 2014. Fully Homomorphic Symmetric Scheme without Bootstrapping. 2014 Int. Conf. Cloud Comput. Internet Things (CCIOT 2014) Fully, no. Cciot, pp. 14-17.

[3] S. R. Ahemad. 2017. An efficient approach based on identity for distributed data possession in multicloud using SelCSP framework. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. pp. 1-4.

[4] I. G. A.; H. M. Leena. 2017. Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud. 2017 World Congr. Comput. Commun. Technol. pp. 172-175.

[5] Viney Pal Bansal; Sandeep Singh. 2015. A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs. 2015 2nd Int. Conf. Recent Adv. Eng. Comput. Sci., no. December, pp. 1-5.

[6] A. R. Buchade. 2014. Key Management for Cloud Data Storage: Methods and Comparisons. 2014 Fourth Int. Conf. Adv. Comput. Commun. Technol. Key.

[7] A. E.-Y.; M. D. E.-C. El Kettani. 2018. Evaluating AND Gates Over Encrypted Data in Cloud Computing. 2018 Int. Conf. Adv. Commun. Technol. Netw. pp. 1-8.

[8] M. W. Fakhr. 2017. A Multi-Key Compressed Sensing and Machine Learning Privacy Preserving Computing Scheme. 5th Int. Symp. Comput. Bus. Intell. A. pp. 75-80.

[9] C. Fan. 2011. Controllable Privacy Preserving Search Based on Symmetric Predicate Encryption in Cloud Storage. 2011 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. pp. 269-273.

[10] A. K. B. H.; S. Soma. 2017. A robust and secured cloud based distributed biometric system using symmetric key cryptography and microsoft cognitive API. 2017 Int. Conf. Comput. Methodol. Commun. pp. 225-229.

[11] Q. B. H.; J. P. Dichter. 2016. Data leakage preventation using homomorphic encryptionin cloud computing. 2016 IEEE Long Isl. Syst. Appl. Technol. Conf. pp. 1-5.

[12] M. R. A.; H. C.; X. Huang. 2014. Smart Integration of Cloud Computing and MCMC based Secured WSN to Monitor Environment. 2014 4th Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. pp. 1-5.

[13] N. Jayapandian. 2016. Enhanced Cloud Security Framework To Confirm Data Security on Asymmetric And Symmetric Key Encryption. 2016 World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave). pp. 1-4.

[14] C. Jeyanthy; R. S. Shaji; J. P. Jayan. 2015. Symmetric key based cryptic scheme for mobile cloud storage. 2015 Glob. Conf. Commun. Technol. pp. 571-575.

[15] S. Kaushik. 2016. Cloud data security with hybrid symmetric encryption. 2016 Int. Conf. Comput. Tech. Inf. Commun. Technol. pp. 636-640.