International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 10 Issue 5, May, 2021, Impact Factor: 7.751

Addressing Data Security in Cloud Computing

Diksha Bisht[1], Purnima Kalia[2], Dr. Banita[3]

[1,2] Research Scholar, Department of Computer Science and Engineering, PDM University
[3]Assistant Professor, Department of Computer Science and Engineering, PDM University

ABSTRACT

Cloud computing area is being evolved a lot of big alterations now a days. A number of business are switching towards cloud computing due to its benefits like anytime-anywhere access, diminishes expenses and loss prevention etc. The data which is being used will be saved on the servers and requires high degree of privacy and authentication hence the main concern of the study is the security of the data. When we upload any data into cloud, we are transferring the control of that data to a third party/person that raises a security concern. The field of cloud computing is not just limited to data getting uploaded on the cloud but it is also used in banking area, hospital management, prediction of security level and mobile application data stored on cloud. The major issue with all the uploading, storing and maintenance of the data is its protection. One of important approach or method to secure and protect the data is encryption that is done using various algorithms to encrypt the data or steganography which helps to protect the data. The study focus on the analysis of various methods which are used to protect data even when it is saved in the cloud itself. For analysis of AES, Blowfish, RSA, 3DES algorithm and extending the areas of cloud computing is discussed in this study.

Keywords: Cloud Computing, Blow Fish Algorithm, Mobile Cloud Computing, Advanced Encryption Standards (AES), Fog Computing

INTRODUCTION

Cloud Computing helps user to take benefit from all the technologies in such a way so that data will remain confidential. Cloud Computing acts as a system where we store the data on remote servers that can be accessed over the internet anytime from anywhere.[1] This can be split into two parts : front-end and back-end.

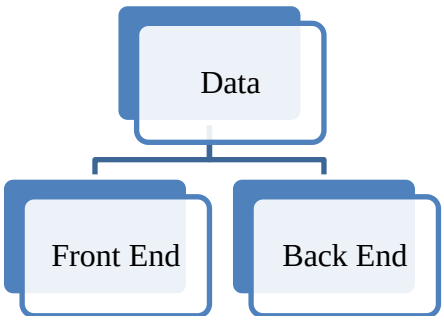

Fig.1 Data used in Cloud Computing

The front-end allows people to view data collected in the cloud using a browser or cloud storage applications. The back-end is responsible for safe and secure storing of data and information. Security and privacy play a important role in Cloud Computing [1]. Although Cloud Computing has a few characteristics that are shared like standard administration and utilization based estimating [2]. Many companies/businesses are migrating to cloud computing due to its various advantages like cost reduction, efficiency, data security, scalability, mobility etc. The data and information could be stored on servers (virtual or physical) is managed and operated by cloud service provider and as a user may use the stored data. Client can get together with the cloud to get dynamically reliable services, such that data can be accessed anywhere and at any time [3].

It is designed to control traffic and customer requests and ensure that all is running smoothly. This pursue a set of guidelines called protocols and uses specific form of program called middle ware. Middle ware enables the communication between networked computers. If the CPS (cloud service provider) has many clients, storage space would like to be high in demand. A physical server maybe fooled into thinking that there are several servers where each running on their own different operating system. This technique reduces the requirement for physical machine, and is called Server Virtualization. It method maximizes single server efficiency.

Cloud computing can be broken into three services. It has been shown in fig.2.

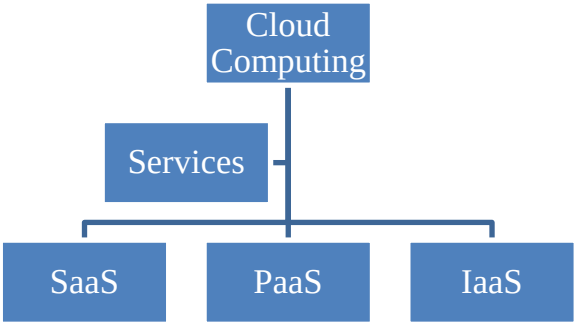

Fig.2 Services of Cloud Computing

- SaaS (Software as a service)
- PaaS (Platform as a service)
- Iaas(Infrastructure as a service)

SaaS is at the top of the stack as users mainly deal with cloud-hosted software, and not the network or infrastructure it operates on.

PaaS permits applications to be developed and implemented by users. Design platforms can be reached as long as an internet connection exists, enabling team members to remain linked and to c ontinue to function.

IaaS is basically the cloud-powered infrastructure and hardware. It allows the users to rent the infrastructure that includes server, data central space, and software. Following are the types of Cloud Computing.

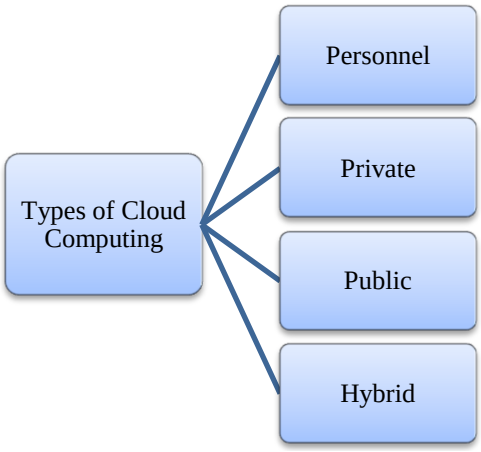

Fig.3 Types of Cloud Computing

There are four types of cloud computing [1] as mentioned in fig.3.

a) ***Personal cloud:*** It is a collection of digital content and services that can be accessed by any device. It offers users the ability to store, stream and exchange the content from one platform to another, screen and location.

b) ***Private cloud:*** It is a paradigm of computing that provides a platform dedicated to a single organization. Private cloud offers virtualized resources for computing through physical components stored on premises.

c) ***Public cloud:*** It includes the services provided via public internet by a third party making them accessible to whoever wants to use the computing service, it can be paid or free.

d) ***Hybrid cloud:*** Its private and public components are linked together but still remain separate entities. This allows to simultaneously deliver the advantages of multiple deployment model.

Besides having so many advantages Security and Privacy of data and information is still a major concern. Storage related issues are Confidentiality, Integrity, and Availability. The main method through which this can be done is encryption. It can be done using different algorithms like AES, Blowfish, RSA, 3DES, Diffie-Hellman, and digital signatures can also be used.

Not just encrypting and decrypting the data, cloud computing area has widened. It is used in banking sector but it is facing issues as the failure rate is high. Here, ANN (Artificial Neural Network) and LMBP (Levenberg-Marquardt based Back Propagation) are used to predict the security level. The aim of cloud risk management is identification and evaluation of cloud security issues at an early stage to predict cloud computing security level[3]. In Hospital management also cloud computing is used and the aim is to offer security on client's data. To achieve the same it uses OTP (One Time Password) while logging in and Blowfish algorithm because it is flexible and mainly for password protection which helps to protect the data and make the data confidential enough [4].

Mobile Cloud Computing (MCC) is a combination of mobile computing and cloud computing, it is like extending the capabilities of mobile. The transmission of off loadable threads (in mobile) is securely done with the help of SHA-256,AES, and Diffie-Hellman. Energy efficiency offloading algorithm is used to minimize the energy consumption. Images present in data can be protected by using steganography, in which key is embedded along with the data has been used to provide extra protection, this can be concluded as data hiding.

Fog Computing Security: It is an extension to cloud computing rather than its replacement. It not only provides storage, resources, networking but also a platform for IoT. This also faces many security issues like malware protection, authentication and trust issues etc. so the advancement in security mechanisms is necessary.

BLOWFISH ALGORITHM

The need to protect the data and take measures to increase security is necessary in cloud computing. Encryption is one of the effective methods to do the same. Here, we are going to get familiar with the algorithm called Blowfish. It was given by Bruce Schneier in 1993 and is mainly used by the general public(users). It has various advantages like it is fast, compact that requires less memory, simple because basic operations are used like XOR, secure and said to be better than DES and IDEA.

Blowfish algorithm can encrypt 64-bit block by using variable length key of size 32 bits-448 bits.

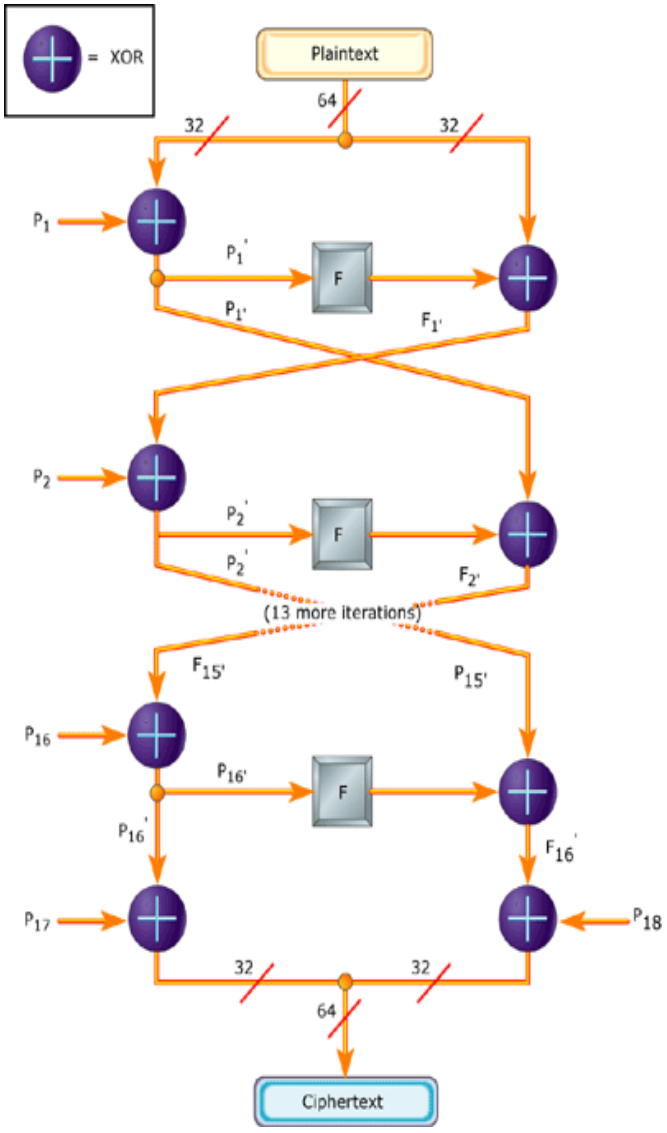

Fig.4 Working of Blowfish Algorithm [10]

During the working of Blow-fish Algorithm fig.4, Sub-key generation takes place, key must be generated before encryption and decryption. Key is taken in the form of an array like K1, K2, ---, Kn [$1 \leq n \leq 14$] of 32 bits each. P-Array is initialized in the same way P1,P2 ,----,Pn , n=18 of 32 bits each and 4-S boxes are generated of 25632-bit entries each of them having S0,----,Sn, n=255. Both P-array and S-boxes have values initialized as hexadecimal form of pi.

Plain text (PT) of 64-bits into two 32-bits texts and operations like XOR and exchange of values are performed accordingly till the last entry of P-Array and we get a Cipher text of 64-bits as a result. In function 'F' of Blowfish algorithm output from first XOR is divided into 4 parts of 8-bit. First is taken and passed through S- Box1, then its result is XOR with second part and S-Box2 and so on. At last, output of 32-bits is sent to be XOR with plain text of 32-bits.

MOBILE CLOUD COMPUTING

Mobile Cloud Computing (MCC) is a technique of processing and storing of data in cloud and using mobile for media display. MCC is the combination of cloud computing and wireless networks [8]. MCC refers to the computing paradigm that combines the capability of low end computing devices like smart phones with the capabilities provided by the cloud computing using network connectivity [6]. It has various advantages like increase in battery life, lesser load on the device, more storage capacity and increase in reliability. Here, also privacy and security is a major concern.

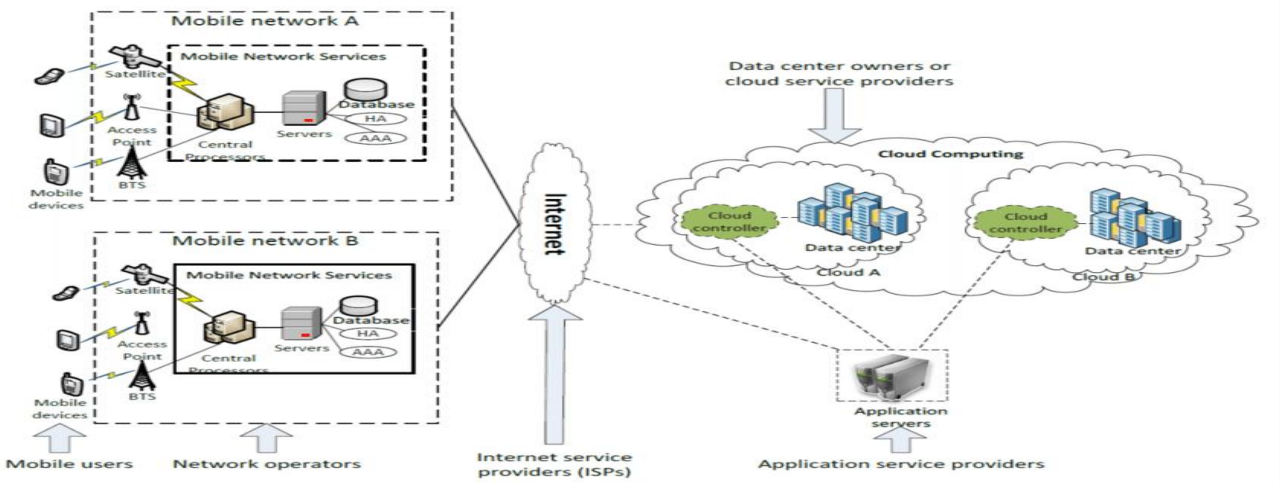

Fig.5 Mobile Cloud Computing Architecture [11]

To have a secure transmission between cloud and mobile various algorithms like AES, SHA-256 and Diffie-Hellman are used. The off loadable threads, wrapped in device are added to the hash value generated by SHA-256. Re-encryption is done by using AES and then, SHA-256 in this. Key generation and digital signatures are used for Diffie-Hellman algorithm and authentication respectively. When the user wants to upload a file, first key is exchanged using Diffie-Hellman, at the time of logging in and the client/user is authenticated using digital signatures. Finally, the data is encrypted using hybrid encryption algorithm and uploaded to cloud.

During downloading some data, as user logins, the encryption keys are exchanged, the file to be downloaded is selected, authentication is done using digital signatures. AES and SHA-256 algorithms are used to decrypt the file selected and then the client/user is allowed to access.

- **AES (Advanced Encryption Standards)**

Cloud Computing is a collection of IT services offered to a customer over a network and these services are distributed by the infrastructure-owned third-party provider. This needs a high standard of privacy and authentication. One of the essential methods is to encrypt the data in the Cloud database server (cryptography). To protect the data, cryptography provides various symmetric and asymmetric algorithms. Symmetric algo has same key for encryption & decryption. Symmetric cryptosystem has the speed and computational efficiency to handle encryption of large volumes of data. In symmetric crypto systems, the longer the key length, the stronger the encryption.

AES is an iterative rather than Fiestel cipher [5]. AES is a type of symmetric Algorithm. It was developed by 2 Belgian cryptographers Joan Daemen and Vincent Rijme.

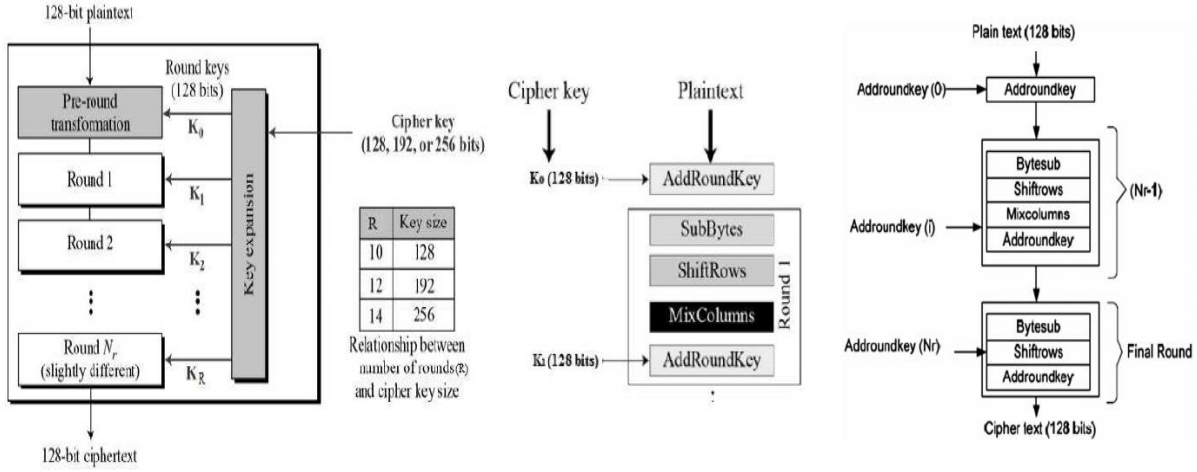

Fig.6 AES Encryption [12]

AES is the most frequent used encryption algorithm and is based on "substitution-permutation network". AES is the fastest method that has the flexibility and scalability and it is easily implemented. AES has very high security as it uses bytes rather than bits to perform all its computations. Hence AES consider the 128 bits of plaintext block as 16 bytes. These sixteen bytes are divided in four columns and four rows for matrix processing. In AES the no. of rounds depends on the length of the key.

AES exhibits resistance to a number of attacks such as square attacks, key attacks, key recovery attack, etc. Hence, the AES algorithm is an extremely reliable method of encryption. Often, data can defend against potential attacks, including smash attacks. AES encryption algorithm has minimal storage space and high efficiency without any drawbacks and limitations while other symmetric algorithms have some shortcomings and variations in output and storage space.

- **Fog Computing**

Cloud Computing provides many benefits for individuals and organizations by offering widely accessible and effective computing services at an affordable rate. Many cloud services are available in current commercial solutions, but are not suitable for latency, portability and location-sensitive applications such as IoT, Wearable Computing, Smart Grids, Connected Vehicles and Software-Defined-Networks. These applications produce vast quantities of varied data at high speeds and, by the time data enters a cloud storage network for analysis, the ability to notify the IoT device to take corrective action may be gone.

Fog computing is a new paradigm, initially and formally introduced by Cisco that expands the architecture of the cloud platform by making computing resources accessible on the edges of a network.

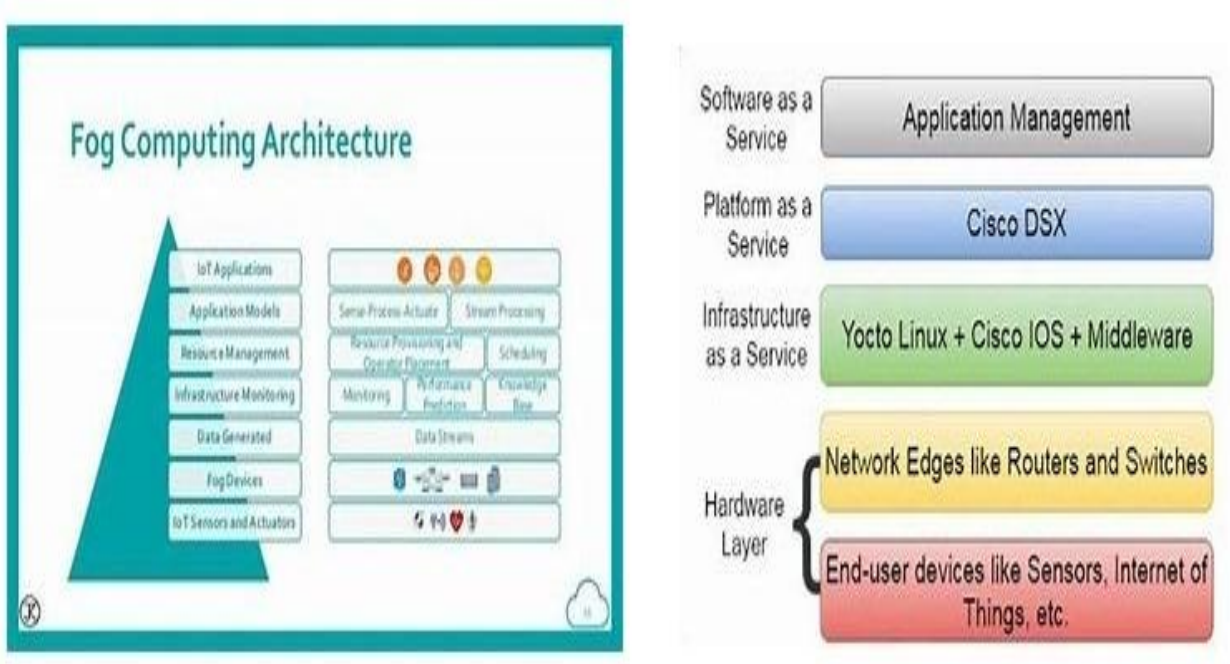

Fig.7 Technical Architecture of Fog Computing [7]

It can be defined as a cloud-like platform that has similar data, processing, storage, and application services, but is fundamentally different in that it is decentralized. However, Fog systems can process large volumes of data locally, run on site, are completely scalable and can be mounted on heterogeneous hardware. These features make the Fog platform highly appropriate for applications that are time- and location sensitive. Fog computing solves the inadequacies of cloud-only models, which have serious challenges with latency, network bandwidth, geographic focus, reliability and security.

Cisco pioneered the Fog computing model delivery, which expands and takes the cloud platform closer to the end-user computer to solve the above-mentioned problems.

Although the word Fog computing was originally coined by Cisco, similar concepts were researched and developed by various other parties like Edge Computing, Cloudlet, Micro-data centre [7]. In a Fog network, both safety and performance factors are considered in conjunction, and mechanism such as the encryption methodologies known as fully homomorphic and cab be used to protect the data somewhat homomorphic. These schemes consist of a combination of algorithms for

symmetric and public-key encryption, as well as other variants for attribute-based encryption. As homomorphic encryption enables normal operations without decrypting the data, every key distribution would maintain data privacy.

Table1. Comparison between various techniques used in Cloud Computing Security with outcomes

S.No.	Work	Methodology	Outcomes
1	Vishal R. Pancholi [1]	• Advanced Encryption Standard (AES)	AES Algo is a highly secure encryption method and shows resistance against various attacks, It is fastest with min. storage space & high performance without any weaknesses.
2	A Venkatesh et.al. [2]	• CSP's Service- Level Agreement (SLA)	Availability should be encapsulated in a CSP's Service- Level Agreement (SLA) to its customers.
3	AbdelrafeElzamly et.al. [3]	• Artificial Neural Network (ANNs) • Levenberg–Marquardt based Back Propagation (LMBP) Algorithms.	ANN is used more efficiently to enhance performance. LMBP algorithms are very efficiently for testing and training networks.
4	M. Sasikala et.al. [4]	• RAS, AES, 3DES, DES • Diffie-Hellman Blowfish	Impact relies upon whether we can build up its qualities and maintain a strategic distance from its detriments.
5	B. Karthikeyan et.al.[5]	• Secured Hashing Algorithm (SHA)-256 • Diffie-Hellman key exchange	The proposed algorithm provides better security when compared with other security algorithms and exhibits better energy efficiency.
6	SuvenduKuila et.al. [6]	• Blowfish Encryption Algorithm • Synchronization&Asynchronous Challenge-Response	Using blowfish algorithm to transfer the information is faster than the other encryption algorithm
7	M. Arunadevi et.al. [7]	• Tripel DES, IDEA Algo • Diffie Hellman Key Exchange	It was only review paper.
8	Hassan Reza et.al. [8]	• Steganography Application • Mobile Cloud Computing Application	The proposed system will work perfectly as long as a user remembers the key
9.	SaadKhan et.al. [9]	• Edge computing, Cloudlets • Micro-datacenters	Most Fog applications do not consider security as part of system, results in many Fog platforms being vulnerable.

CONCLUSION

Cloud Computing technology is emerging, for many years it has given various benefits to different organizations. Many businesses are adapting to cloud computing. Since, this is still growing, security plays a very significant role. So, one of the method to maintain confidentiality, integrity, and provide protection is encryption. In this study, two main algorithms that are Blowfish and AES, which are said to be very effective were discussed. Both of them are in demand but if we compare Blowfish and AES algorithm then Blowfish is said to be better than AES, because it is faster and does not have any security weak points so far. MCC is also trendy right now, as the processing/storage is done on server. To protect the data, a combination of different algorithms like AES, SHA-256 & Deffie-hellman is used. Cloud computing is not suitable for some applications like IOT and for this Fog Computing Security is used. It not only provides storage resources ,networking but also platform for IOT. It is an extension to cloud computing rather than its replacement.

REFERENCES

[1] A Venkatesh, Marrynal S Eastaff, "A Study of Data Storage Security Issues in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), publishes in 2018 ,Volume 3, Issue 1, ISSN : 2456-3307.

[2] M. Sasikala, Dr. v. Anuratha, "Analysis on Cloud Computing Security Issues and Algorithms", International Journal for Research in Science Engineering Technology (IJRSET), published in January 2017,Volume 4, Issue 1.

[3] M. Arunadevi, Dr. V. Sathya, "Analysis on Cloud Computing Security Algorithms and Its Security Challenges", International Journal of Computer Science Engineering and Technology (IJCSET), published in April 2018, Volume 4, Issue 1.

[4] Suvendu Kuila, Shruthi Shridhar, Chandan Patel, N. Ch. S.N Iyengar, "Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management", International Research Journal of Computer and Mathematics Science, published in November 2016, Volume7(11).
[5] Vishal R. Pancholi, "Enhancement of Cloud Computing Security with Secure Data Storage using AES", International Journal for Innovative Research in Science & Technology(IJIRST), published in February 2016, Volume 2, Issue 09.
[6] Hassan Reza, Madhuri Sonawane, "Enhancing Mobile Cloud Computing Security Using Steganography", Journal of Information Security, published on 19 July 2016.
[7] SaadKhan, Simon Parkinson, YongruiQin, "Fog computing security: a review of current applications and security solution", Journal of Cloud Computing: Advances, Systems and Applications, published in 2017.
[8] B. Karthikeyan, T. Sasikala, S. Baghavathi Priya, "Key Exchange Techniques Based on Secured Energy Efficiency in Mobile Cloud Computing", International Journal Applied Mathematics and Information Sciences, 1 November 2019.
[9] Abdelrafe Elzamly, Burairah Hussin, Samy S. Abu Naser, Tadahiro Shibutani, Mohamed Doheir, "Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations", Information Technology and Electrical Engineering (ITEE), published in April 2017, Volume 6, Issue 2.
[10] Bliff Gatliff, " Encryption data with the Blowfish algorithm", July 2013, www.embedded.com.
[11] Hoang T.Dinh et.al. , "A Survey of mobile cloud computing: Architecture, applications and approaches, 1587-1611, 2011.
[12] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm