EasyChair Preprint

№ 3667

A Descriptive Study on Emerging Methods for Data Security in Cloud Computing

Srinidhi Kulkarni and Muktikanta Sahu

June 22, 2020

A Descriptive Study on Emerging Methods for Data Security in Cloud Computing

Srinidhi Kulkarni, Prof. Muktikanta Sahu

Department of Computer Science and Engineering

International Institute of Information Technology, Bhubaneswar

Email Id: <b417034, b417047, muktikanta>@iiit-bh.ac.in

Abstract:- In this paper we did a literature study of the security algorithms that have been proposed to secure the Cloud computing platforms. The paper presents the potential threats, security issues of cloud computing platforms and the efficient research work carried out on these fields. The cryptography based security algorithms such as RSA, DES, AES, ECC and BLOWFISH have been discussed and the works relating to these algorithms were also studied and their results are presented. Some novel approaches in which Machine Learning frameworks were used to enforce the security of the cloud are also mentioned and discussed in detail. A comparative study of the security algorithms based on their performance on various impact factors of a system is also presented based on the research of the past. The discussion in this paper is a generalized discussion which is applicable to any service and any type of deployment of the cloud computing system. The paper aims to contribute to the domain knowledge of security and the different ways to enhance it.

Keywords- Cloud computing, Security threats and breaches, Cryptography, Security Algorithms, Machine Learning

I.INTRODUCTION

Cloud computing is a newly emerged technology with extensive scope of advancement. Initially the time sharing concept based data centers assigned the tasks(jobs) to the mainframe of the companies. As the technology advanced, the companies began using VPN based networks. The general notion was thought the demarcation in such systems between the end users and the servers was a cloud. With experimentations and using more optimized algorithms the computing power and scalability of this cloud was further expanded, this was the beginning of the cloud computing revolution. The main notion of introducing this technology was the efficient usage of the resources for the end user even at a lower bandwidth [2][3][5]. Many believe that the idea of providing computation as a utility was for the first time proposed by scientist John McCarthy [27] . Cloud mainly offers the service of storing and providing on-demand access to the data over the internet. The usage of the cloud services is increasing exponentially as the contemporary paradigm of technology is about the data revolution. The main attributes of the cloud are Multitenancy, scalability, Elasticity, being more user-friendly. Now the focus of the cloud services is mainly on making it more user-friendly. In order to do this we need to take care that the user is less bothered about the technicalities related to the structure and working of the cloud and make it a more secure platform for the

user's huge amount of data. In order to increase the quality of the services and infrastructure provided by the cloud, its attributes need to be expanded. But these expansions can lead to compromising on the security matters. Every cloud service provider has to take care that the client hosts data to the cloud and there should be some certainty with regards to the access to that data that it will be only limited to the authorized access. The clients data safety and proper practices and privacy policies are to be validated to assure the cloud users of the data safety and privacy protection.Security and privacy is a key aspect as with the growing technology we also end up bearing cost for that. As all the cloud interactions need an internet connection as the internet becomes the path of our data transmission its unauthorized nature can cause trouble to the integrity of the data. Today there are many intruders and hackers that try to intrude the CSP firewall and steal or hamper the users data. This data breach can be very costly to the user as well as the CSP as the data out there through static or in transmission is valuable and of great use.Based on the hacking motives, various researchers have also proposed a variety of techniques to protect the security of data during transmission. The type of mechanism used for protection depends on the size and nature of the data. In recent times the hacking has also turned out to be a profession from time to time that NIST organises events or competitions in which the different security schemes are attacked and based on the results the best ones are decided and the loopholes of the other algorithms are noted. So when we look at these scenarios we realise that the need for security is alarming and there is a need that we change the perspective towards security and make it more broaders and protect systems from attacks or intruders. There has been a lot of discussion about the way the security issues are looked at should be changed and more matured emphasis should be laid on this matter[28].

In this survey, The section 2 gives us clarity about the different security issues involved in the CSP to user communication and why it seems vital to deal with them.The section 3 introduces us to the security algorithms and the works done based on them. In section 4, We try to have a basic comparison between the algorithms based on the information and knowledge gathered from the regrees. In section 5 we conclude the paper with the acknowledgments as the section 6.

II.FACTORS RELATING TO THE SECURITY ISSUES

Virtualization:

It is the process of creating a virtual version or a virtual platform of a server, a device or a resource. In simple terms it is the logical division that can help in usage of resources and services by time sharing. Generally to felicitate the process of the virtualization the hypervisors are involved on the host machines to run the guest operating systems. So it is very important that the hypervisor is not vulnerable because the failure in proper functioning of the hypervisor can lead to the collapse of the entire process and thus endanger the data. Another risk involved here is that if the hypervisor fails to maintain a proper mechanism to maintain the allocation and deallocation of the resources then there a possibility that after one of the Virtual Machines access is ceased and if the resources are still available on the system then it can be available to the next VM that is running and these prior resources to the current may be of no importance but in this scenario the data is available to a VM(Virtual machine-Guest machine) which has no need of it so there can be a case of data privacy disruption. There can be many security and privacy breaches in the data at the virtualization level [30].

This can be resolved by having a strong authentication before allocation and deallocation of the resources.

Multitenancy:

The resources are shared between multiple users simultaneously. So there is a possibility that the private data of one user gets leaked and can be accessible by any other user. And this condition can be very sensitive to the motives of the hackers. So it is important to authenticate the users before providing them the access to the cloud resources.

Stativity and Transitivity of Data:

The data stored in the cloud is static and as it remains in the cloud for a longer time it is important to keep the integrity of the data intact.For data that flows from and into the cloud is called the transit data. The main transit data is the usernames and passwords that always flows to the cloud whenever there is request access. So the data while passing through the network for the authentication is to be protected and this can be done using the various encryption techniques.

Location Transparency:

The resources are recognized based on the way the network is configured rather than based on its physical location. But this can be dangerous to the security that the intruders can change the network settings.

Interoperability:

Interoperability can be defined as the different cloud systems can collaborate and connect to work together. It also means the inter-connected systems can also have an access over each other's data services as well they tend to have an understanding of the other systems authentication methodologies, formats etc. And as times are growing the demand for the inter connected clouds is increasing so there is an urgent need to respond to this security issues of interoperability to ensure the safe intercloud systems[29].

III.SECURITY ALGORITHM

Cryptographic Algorithms:

In this comparative review of cryptography algorithms, we have focused on some very popular algorithms: RSA, ECC, MD5, AES, DES. There are mainly two types of security algorithms:

- **Secret-Key Cryptography (SKC)**
  (Symmetric encryption)
- **Public-Key Cryptography (PKC)**
  (asymmetric encryption)

SKC uses a single key that is used for encryption as well as decryption of data. On the other hand, PKC uses two types of keys : public-key, private-key. Public key is used by cloud service providers for encrypting the user data and is known to all, whereas private-key is used by users for decrypting the encrypted data back into its real form, this key is offered privately by cloud service providers to a user using the cloud service. Secret-key algorithms are also called symmetric algorithms while Public-key algorithms are also called as asymmetric algorithms. In this section, we have put light on briefly describing how these algorithms play a role in encrypting the data to be stored in the cloud. The functioning of these popular algorithms are briefly described below:

Secret-Key Cryptography (SKC):

In these types of the algorithm there is only a single key involved at the time of encryption as well as decryption. This is the symmetric key that stays with both the CSP as well as the user. So, the main challenge here is the distribution of the keys. As this cannot be ensured that there will be secure transfer of the keys over an unsecure channel. And as there are no unique keys to the user as well as to the CSP it's difficult to keep a track of the transactions of the data. We can just identify the activity but not have a clear idea of what action was done by whom in the data transaction process.

1. AES: In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard which can be further extended to be used in cloud data security. It was established by NIST in 2001. Each of the ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES algorithm came up as a complementary algorithm to the DES as its working mechanism was similar but the prior one performed better on the security standards compared to the later one. AES is an algorithm that can be implemented at both hardware as well as the software levels. This algorithm provides a lot of scope for developers as well as the researchers to make the mathematical changes in the algorithm to make it deployable for the service requirement.

Vishwanath S Mahalle et al [14] proposed and implemented a security system based on the RSA and AES algorithms as this was a hybrid cryptography based system its performance was better than the pure cryptographic systems based solely either on RSA or AES.

2. DES: DES stands for Data Encryption Standards. It is one of the popular encryption algorithms. It operates 64-bit sized plain text blocks and returns ciphertext blocks of the same size. The key-length is initially 64 bits but as the algorithm processes, every 8th bit is discarded to form 56 bits long key. This has 4 modes of operations.This is implemented based on the Feistel block ciphers [20]. 1n this method the permutations of the texts is tried and form boxes on which various rounds of encryption is performed .This method is vulnerable to many powerful attacks.

Zameer Fatima et al [21] proposed a system in which the audio steganography was carried out by building a model based on the DES algorithm. In this work the audio is first encrypted using the DES algorithm and then from the encrypted text every LSB of each byte is made zero. The entire information of the 8 bits is hidden in the LSB. In the encoding stage first the size of the audio file is encoded based on this number the decoder fetches that many numbers of corresponding LSB bits from the remaining length of the data. The gathered LSB bits are decoded and then the message is decrypted for the original message. The result is that a secured level of steganography is done of the audio but the quality is highly dependent on the size of the audio file. This kind of steganography can also be used for storing the data on the cloud server.

3. BLOWFISH: Blowfish [1] is a symmetric key block cipher, designed in 1993 by Schneier. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It uses a feistel cipher block of 16 rounds which has very large key based s-boxes.

Public-Key Cryptography (PKC):

This type of cryptography was mainly developed to have a two party communication i.e by having a secure communication over an unsecure channel via the proper encryption of the randomly generated session keys that are encrypted generally using the public key and decrypted using the private key. Both the keys are somewhere mathematically associated. But having one key will not make it feasible to know the other key. The kind of mathematical functions involved are of such a nature that it's very difficult to find their inverse so hence that is why instead of using one key we use two different keys.

As we use two different keys it's easy to have a track on transactions done on the cloud as the processes of encryption and decryptions are done by separate keys.

4. RSA:This was the algorithm proposed by three mathematicians Ron Rivest, Adi Shamir and Len Adleman in 1977 . This algorithm is named as RSA based on the First letters of the name of the authors.This algorithm is mainly used in the systems where the system needs to exchange the symmetric keys or in a case of the digital signature authentications. RSA is an asymmetric and Public-Key algorithm. RSA is a block cipher, It takes place in three steps: Key-generation,Encryption, Decryption. NIST recommends using 2048 bits long keys for RSA. This is a homomorphic encryption scheme with regards to the arithmetic operations. That implies if any such arithmetic operations are done then the changes can be done to the text without decrypting the text and directly to the cipher texts. And the result is another cipher text which on decoding is equal to the operations carried on the plain text[23]. Nowadays the issues regarding cloud safety increases it has become that the security systems are now designed on the concepts of Homomorphic schemes as the data can be decrypted only by the owner of the private key. That means this approach can be an ideal one for the Cloud Environments as the data transfers as well as access to desired data can be provided in the encrypted form. So that the potential risk of the plain text being accessible to the intruder can be controlled. But there have been recent times whether the scope of the homomorphic encryption has increased its range to the logical operations as well as shown and proposed by Yi-Fan Tseng et al [22] in which the Composite order bilinear groups are used for making the scheme homomorphic with regards to the logical operations such as AND and OR operators.The plain text is first converted into its ASCII values later converted into its bit string. And this bit string is now treated as a decimal number 'M' which is generally a very big number.

Parsi Kalpana et al [4] showed how to encrypt data using RSA in her work.The keys are generated as follows:

Steps:

1. Select two distinct primes a and b such that they are chosen randomly and are of same length.
2. Calculate the value of n=(a*b)
3. Compute the euler's totient function i.e
   $\boldsymbol{\Phi}(n)=(a-1)*(b-1)$
4. Choose a random integer 'e' such that it lies between 1 and $\boldsymbol{\Phi}(n)$ such that the gcd(e,$\boldsymbol{\Phi}(n)$)=1.
   Here 'e' is termed as the public key exponent.
5. Now compute the value of $d=e^{-1} \pmod{\boldsymbol{\Phi}(n)}$ i.e d is the multiplicative inverse of e mod $\boldsymbol{\Phi}(n)$.
6. 'D' is a component of the private key.
   So that $d*e=1 \bmod \boldsymbol{\Phi}(n)$.
7. Public key is a tuple of modulus n and the public exponent i.e, (e,n).
8. The private key is a tuple of modulus n and the private exponent i.e,(d,n).

The encryption is done as:

$C=M^e \bmod n$

The decryption is done as:

$M=C^d \bmod n$

The encryption and decryption are both based on the integer numbers.

Vishwanath S Mahalle et al [14] showed implementing a security system based on RSA on a cloud service provider. In this work, the security system is implemented in two modules: Uploading and Downloading.Where a key generation mechanism was designed to have a secret key based on RSA and AES . The keys stayed with the user and asked for keys whenever the user intends to upload or download the authentication is done based on these keys.

S. Selvakumar et al [31] proposed a method in which an algorithm for padding was called the Optimal Asymmetric Encryption Padding (OAEP) is used along with the RSA algorithm to improve

its security standards of the system. This model concludes that the OAEP resists the attack on the cipher texts.

The main application of this algorithm is used nowadays to encrypt the session keys generated at random by the systems that are supported by the SKC or hash function based security algorithms i.e example in simple terms the public private keys are used to protect the process of distribution of the symmetric keys if the system has a SKC based security system. This algorithm works efficiently because the chosen p and q are very big hence its very difficult to computationally evaluate the public key and the private key just out of the 'n' as finding the prime factors of such a big number is computationally very costly. The problem of finding the prime factors for a given large number complexity wise is a hard problem.

5. ECC: ECC is an asymmetric cryptography algorithm. The algorithms proposed before were mainly the RSA based once i.e based on the IFP problem. But as the technology is advancing we need more stronger algorithms. Then came few algorithms that were based on more stronger and complex mathematical concepts like the discrete logarithmic problems (DLP) based EIgamal Cryptosystems[19] but later the need arises for more stronger system so lead to the the focus of the cryptographers to the mathematics of the Elliptic curves.

ECC(Elliptic Curve Cryptography) is based on the mathematical problem of Elliptic curve Discrete Logarithm Problem(ECDLP) that is more complex to solve than the Integer Factorization Problem (IFP) or DLP. And yet there is no exponentially computationally viable method to find a solution to the ECDLP based problems. Even in this there are two keys involved. I.e the public key and the private key.

Comparatively to the other types of PKC algorithms proposed until then ECC proved to be more efficient than them. It is a variable length based key encryption algorithm. And the major advantage was that the ECC consumed shorter bandwidth for transmitting smaller sized encrypted messages. So the bandwidth is saved which in turn assures that the data probability of the data being lost is less.[18]

Alowolodu O.D et al. [5] in his work suggested a way of using ECC for securing the data over cloud platforms.

Syam Kumar P et al [15] proposed a work in which the integrity of the data stored in the cloud was verified based on the ECC and Sobol Techniques. This work used the approach of Secure storage to check the integrity of the data blocks by picking them randomly from the cloud server. Here the model involves a third party verifier except the user and CSR which checks for the integrity and security of the data on the behalf of the users as most of the users lack the technical knowledge. This method is more user friendly as well as more secure.

Machine Learning Based Approaches:

The use of machine Learning Algorithms is generally carried for data processing. But the usage of the algorithms for the security purpose was something that can be considered as a novel approach that unites the domain of Machine Learning and Data Security. As the computational capabilities of the computers increase it becomes easy to resolve and find the solutions to the computationally hard problems which are the basis of the cryptographic security algorithms. So we need to find newer methodologies where we are dependent on the security approaches which are not based on mathematical functional operations but rather focussing on the pattern in which the data is stored rather than just creating cipher texts to store rather try to learn the pattern of the data and store it in a different format and reconstruction of the data is possible based on the learnt knowledge. So in these kinds of approaches Machine Learning can serve as the technology that protects our data in a newer way. Another way it plays a role in security is in applying the machine learning principles on the encrypted texts or a hybrid security system where both Machine Learning or cryptography together reinforce the security aspects.

The works mentioned below show that security ensuring methodologies enter a new paradigm as latest technologies other than cryptography emerge,suggesting better approaches or efficient security solutions.

Mbarek Marwan et al [16] proposed a model in which the security of the cloud is ensured by segmenting the image into 4 different regions based on the intensity levels and this is carried out by a combination of SVM and FCM. Initially the images are taken and all the pixels are classified into different regions by the SVM linear classifier but as the classifier is mainly intended for supervised learning we combine it with the FCM that trains the SVM to enhance the performance of the linear classifier. The FCM plays an important role in extracting the pixel level color features. These features are the input vectors that are fed to the SVM for the classification purpose. SVM classifies the pixels into different regions. In this way the image is stored to the cloud in its segmented format. This work was carried on the healthcare industry images.

Shalu Mall et al [17] proposed a framework to protect and increase the security levels of the cloud based on the genetic Algorithms. The data is initially converted into the ASCII characters and then the latter are converted into the block of bits. This conversion of the ASCII characters to block of bits is carried out by the data owner(DO). We apply the genetic algorithms randomly to these blocks of bits to encrypt them and output cipher blocks. The genetic algorithm operations such as the cross overs and mutations are applied on these blocks of bits to encrypt them. The type of operations to be carried out is determined by the pseudorandom number generator function.Once the encryption is done these blocks are stored at different locations on the Cloud and further the security of these cipher blocks is strengthened by the DO provided key. Hence this system involves only one key and rest is dependent on the GA. Hence this framework's performance is essentially good. The decryption can be done based on the dynamic urls and reversing the GA based operations carried out and by converting back from ASCII to original text. The GA operates on random blocks of the data as a result this contributes more to the security. In the next section, we have tried comparing these techniques based on their security strength, integrity, execution speed and various parameters but each of these cryptographic approaches has its own benefits and limitations.

The above two references that were cited were mainly about using Machine Learning techniques to ensure security, But a novel approach of training the deep neural networks for them to get trained on the encrypted data and to learn the pattern of the encrypted data itself rather than the original data. The main concept embedded here is the concept of Homomorphic encryption in which any operation performed on the encrypted data generates a cipher text as a result which when decrypted is equal to the result of the same operation performed on the plain text, hence to hold the homomorphic property of the cipher text true we cannot perform complex computation or operations on the cipher texts as proven mathematically [25]. In the paper by Ehsan Hesamifard et at [24] a model based on deep neural networks was trained on the encrypted data and the trained model was used for performing the classification task. Here the deep Neural networks were brought into the range of the homomorphic encryption by approximating the complex activation functions to its polynomial equivalent while preserving the accuracy of the performance of the model. The result of this approach was comparable to those of the Cryptonets rather the proposed system performed better than the Crypto Nets. So this proposed system can resolve the concerns of the risks involved while using the cloud platforms for the analytics tasks. Using the prior mentioned methodology can be vital one in which the analytics can be performed on the Cloud servers while not compromising or loosing the privacy of the data as all the analytics run on the encrypted data and the access to decrypted data isn't required for the analytics.

IV. ANALYSIS & COMPARISON

If we compare the various methods based on their speed discussed above, it is very general statement that asymmetric cryptographic algorithms are a bit slower than symmetric cryptographic algorithms so we can say that ECC, RSA are slower than DES, AES which falls under symmetric category.

This statement is made due to different public and private keys with a longer size of key used in asymmetric algorithms. Similarly, when it comes to security, we can say that all the asymmetric cryptography techniques are more reliable because of the different keys used for encryption and decryption. On the basis of storage capacity, it is true that those algorithms require more storing capacity which have keys of longer lengths. But we cannot generalize the comparison for all algorithms based on general statements. So, let's dive deep into a detailed comparison.

The methods proposed in the tables were implemented and checked for their average time of encryption and decryption.This simulation uses the provided packages in python 3 environment to simulate the performance of DES, AES, RSA and Blowfish implementations. This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The simulations are conducted with a 64 bit processor with 8GB of RAM. The development environment used for the simulations are the Jupyter Notebooks and the Google Colab.Considering different sizes of data blocks (20B to 400B) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data blocks. All the implementations were exact to make sure that the results will be relatively fair and accurate.

A comparison of some of the above mentioned papers has been done based on their time of encryption and decryption on different size of inputs.The results are:

METHOD PROPOSED	**30 Bytes**	**50 bytes**	**100 Bytes**	**200 Bytes**	**400 Bytes**
RSA-OAEP (key:1024 bits)	0.003	0.00312	0.0032	X	X
RSA-OAEP (key:2048 bits)	0.009	0.0103	0.0084	0.0105	X
RSA-OAEP (key:3072 bits)	0.023	0.024	0.021	0.025	X
DES(using audio steganography)	0.776	0.78	0.78	0.79	X
2-tier(RSA+Blowfish)	0.29	0.29	0.29	0.301	0.305
3-tier(RSA+Blowfish+DES)	0.303	0.305	0.31	0.343	0.35
Hybrid system(AES+ECC)	0.0049	0.005	0.0057	0.0057	0.0057

The table shows the aggregate time for encryption and decryption for the methods proposed. The units of time are seconds.

The role of ECC becomes major when the computational power and memory are limited. Moreover, as the size of key increases in RSA, the permutations of cracking the key also increases. Each one of them has its own importance depending upon the computational specifications provided.

Benefits and drawbacks of DES [8]:

Benefits:

The nature of the algorithm is complex, it's not easy to crack the mathematical logic lying in it as at each round the Boxes undergo a permutation-combination phase before undergoing the subsequent rounds of generating the cipher texts.

Sombir Singh et al [8] proved in his paper that DES works better i.e in terms of time taken to encrypt and decrypt the data than compared to RSA. This is proven on different input sized files.

Drawbacks:

As it involves a permutation combination phase, there is a chance that a specific pattern of two inputs may generate the same output. So because of the presence of the permutation and combination phase there is a discrepancy in the initial and the final outputs of the system.

Benefits and drawbacks of RSA [9]:

Benefits:

As it involves the finding of the integer factorization of a larger number it isn't that easy. It is a tedious job which takes a lot of time. So to be on a more secure side the size of the keys should be longer. And though if either of the keys is known even then the other key couldn't be found as they have no simple mathematical relation existing between them.

Drawbacks:

As the computation power of the computers is increasing. And the concepts such as the parallel computing make an exponential growth in the computation abilities and as a result those processes that required a lot of time to get computed can now be done more easily so the way RSA is vulnerable to these breaches as the intruders use the concept of brute force that means to generate all the possible combination of the keys posible and test each, the only way to increase is security is by always having a larger number to find its factors i.e to combat the increasing computing abilities we need to have larger key but maintenance of larger keys is very difficult as the decryption ends up being a very long process.

Benefits and drawbacks of AES [10]:

Benefits:

It is one of the most popular security standards. It can be very easily implemented both in hardware as well as software. Most of the open source solutions use this standard to protect the data. For 256 bit, about 2^{256} attempts are required to break the security standards. This makes it very difficult to hack hence can be said as a very safe protocol.

Drawbacks:

It uses too simple mathematical logic like the simple algebraic structures which makes it more vulnerable to the key scheduled attacks. Hence when we look at the simple mathematical foundation of the algorithm, we can say its easy to invade and intrude into the system protected by this algorithm.

Benefits and drawbacks of ECC [11]:

Benefits:

It can be said to be implemented really fast as the binary curves work really well on the hardware. The significance of this algorithm is that it ensures security with smaller keys and its size of encryption is not fixed i.e the smaller messages generated smaller sized encrypted messages. As the size of the message determines the size of encryption hence it is successful in even utilizing the bandwidth efficiently.

Drawbacks:

Complicated and tricky to implement securely, particularly the standard curves.Standards aren't state-of-the-art, particularly ECDSA which is kind of a hack compared to Schnorr signatures. Signing with a broken random number generator compromises with the key.Still has some patent problems, especially for binary curves. Newer algorithms could theoretically have unknown weaknesses. Binary curves are slightly scary.

Benefits and drawbacks of Blowfish [12][13]:

Benefits:

This is one of the fastest even when it comes to its operation. It can be said to be faster than the DES. The algorithm is the one that works well on small memory spaces. There is a flexibility of the key size. The strength of the algorithm can be made better by increasing the number of rounds.

Drawbacks:

As each of the users has a unique key, so as the number of users increase it becomes more difficult to manage the keys.It also has the weakness in the decryption process over the other algorithms in terms of time consumption and serially in throughput.

V. CONCLUSION:

In this paper various cryptographic methods were discussed to encrypt the data and the different kinds of ciphers were also discussed which can improve the security of the cloud environment irrespective whether the data is static or transit. With emerging new technologies newer approaches also need to be adopted to make the cloud secure as the threats and breaches also get immune to the other approaches. Hence a novel technique of using Machine learning for securing the cloud data was also discussed. A comparison was laid out between the algorithms so that based on the requirement of the cloud systems the appropriate approach can be implemented. In this era of data revolution, there is enormously bulky data out which needs to be processed and stored for which the cloud servers gain the users attention. This makes the privacy and security of the cloud data a vital aspect to have a secured efficient service.

VI. ACKNOWLEDGEMENT:

The first and the second author would like to state that this work is possible mainly because of the opportunity given and the support extended by Prof. Muktikanta Sahu. We thank all the referees for their contribution and works that made us understand and learn the concepts involved to enhance our domain knowledge.

REFERENCES:

[1]. B. Schneier et al., “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994. This paper also appeared as: "The Blowfish Encryption Algorithm," Dr. Dobb's Journal, v.19, n. 4, April 1994

[2]. Griffin, Ry'mone,"Internet Governance. Scientific e-Resources",November 2018 .

[3]. Corbató, Fernando J. "An Experimental Time-Sharing System". SJCC Proceedings. MIT. Retrieved 3 July 2012.

[4]. Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, September 2012.

[5]. Alowolodu O.D, Alese B.K, Adetunmbi A.O., Adewale O.S, Ogundele O.S., "Elliptic Curve Cryptography for Securing Cloud Computing Applications", International Journal of Computer Applications, March 2013.

[6]. Amal Abdulbaqi Maryoosh, Rana Saad Mohammed, Raniah Ali Mustafa, "Subject Review: Cloud Computing Security Based on Cryptography", International Journal of Engineering Research and Advanced Technology (IJERAT), September 2019.

[7]. Gurpreet Kaur, Manish Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms", Int. Journal of Engineering Research and Application, Sep-Oct 2013.

[8].Sombir Singh , Sunil K Maakar and Dr. Sudesh Kumar ,"A Performance Analysis of DES and RSA Cryptography",International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), June 2013.

[9]. NaQi , Wei Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen, Xiaoyan Yin, Xiangrong Xiao and Jie Hu, 2013. Analysis and Research of the RSA Algorithm. Information Techndology Journal, 12: 1818-1824.

[10]. https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html

[11].https://steemit.com/cryptography/@shubhamupadhyay/elliptic-curve-cryptography-or-rsa-algorithm-and-why-or-advantages-and-disadvantages in 2017.

[12]. https://brainly.in/question/1744703 in 2017.

[13]. S. S. Sudha, S. Divya, "Cryptography in Image Using Blowfish Algorithm ",International Journal of Science and Research (IJSR) , 2013.

[14]Vishwanath Mahalle,AniketShahade,. "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm",INPAC ,October 2014.

[15]. Syam Kumar P, Subramanian R,"An Efficient and Secure Protocol For Ensuring Data Storage Security in cloud Computing",November 2011.

[16].Mbarek Marwan, Ali Kartit, Hassan Ouahmane,"Security Enhancement in Healthcare Cloud using Machine Learning", Procedia Computer Science, January 2018.

[17] Shalu Mall,Sushil Kumar Saroj,"A New Security Framework for Cloud Data",Procedia Computer Science, January 2018.

[18]Jia Cui,Yudong Qi, Bei Hong, Qinghua Chen," Research on cloud computing data security based on ECDH and ECC", International Journal of Simulation: Systems, Science and Technology, 2016 .

[19] JaspreetKaur Grewal,"EIGamal:Public-Key Cryptosystem", A paper presented for Masters Degree, Indiana State University, September 2015.

[20] Ayan Mahalanobis, "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups." 2005

[21] Zameer Fatima and Tarun Khanna,"Audio Steganography Using DES Algorithm",INDIACom-BVICAM, March 2011.

[22] Tseng, Yi-Fan and Fan, Chun-I and Kung, Ting-Chuan and Huang, Jheng-Jia and Kuo, Hsin-Nan,"Homomorphic Encryption Supporting Logical Operations", Proceedings of the 2017 International Conference on Telecommunications and Communication Engineering(ICTCE),(2017).

[23] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation" ACM Comput. Surv. 51, 4, Article 79 (September 2018).

[24] Ehsan Hesamifard, Hassan Takabi, Mehdi Ghasemi, and Catherine Jones," Privacy-preserving Machine Learning in Cloud", In Proceedings of the 2017 on Cloud Computing Security Workshop (CCSW '17). Association for Computing Machinery,(2017).

[25] Pengtao Xie, Misha Bilenko, Tom Finley, Ran Gilad-Bachrach, Kristin E. Lauter, and Michael Naehrig. 2014. Crypto-Nets: Neural Networks over Encrypted Data. CoRR abs/1412.6181 (2014)

[27] Rich Miller, "What's In A Name? Utility vs. Cloud vs. Grid". Retrieved September 29, 2009, from Data Center Knowledge: http://www.datacenterknowledge.com/archives/2008/03 /25/whats-in-a-name-utility-vs-cloud-vs-grid/

[28] Vijay Varadharajan. 2011. Rethinking cyber security. In Proceedings of the 4th international conference on Security of information and networks (SIN '11). Association for Computing Machinery, New York, NY, USA, 3–4. DOI:https://doi.org/10.1145/2070425.2070428

[29] Kiranbir Kaur, DR. Sandeep Sharma, and DR. Karanjeet Singh Kahlon. 2017. Interoperability and Portability Approaches in Inter-Connected Clouds: A Review. ACM Comput. Surv. 50, 4, Article 49 (November 2017), 40 pages. DOI:https://doi.org/10.1145/3092698

[30] Rajendra Patil and Chirag Modi. 2019. An Exhaustive Survey on Security Concerns and Solutions at Different Components of Virtualization. ACM Comput. Surv. 52, 1, Article 12 (February 2019), 38 pages. DOI:https://doi.org/10.1145/3287306

[31] S. Selvakumar , Sahil Baid & Vidit K. Shah," SECURE SHARING OF DATA IN PRIVATE CLOUD BY RSA – OAEP ALGORITHM",International Journal of Pure and Applied Mathematics, Volume 115 No. 6 2017, 689-695