An Analysis of AES, RSA and Blowfish-A Review

Mrs. Caroline Kalaiselvi. R[1] , Dr. Mary Vennila.S[2],
[1] Research Scholar, PG and Research Department of computer science, Presidency College, Chennai
[2]Associate Professor, Head & Research Supervisor, PG & Research Department of Computer Science, Presidency College, Chennai.

Abstract-We all know how science encompasses all aspects of our daily life. But science in its various avatars took time to evolve . It is not known to have jump-started in any sphere of its activity. Its evolution was gradual. The same is with computer science too, as it had its restricted use during its initial stage of evolution touching peripherally networking that was put into use by minuscule percentage of the population with absolutely no interference from any outside source. But when computing became the sole refuge of every profession that you can name, ethical as well as unethical practices start impacting wherever computer science started playing a major role. While ethical practices have a positive import to its employment , unethical practices like snooping, stealing data for ulterior motive like defrauding for illegal monetary gain, destabilizing an establishment by sabotaging essential data and the list is endless and very foreboding today, securing the computer data became *sine qua non* and enormous amount of energy and time is spent in updating a foolproof secure system to save and protect data from being breached by inimical sources. Here came encryption as a potent tool to secure data. Let us now delve into an elaborate theoretical study touching upon the DES, 3DES, AES and Blowfish symmetric encryption algorithms. We have drawn a comparison of analysis on the symmetric encryption algorithms. However this process proves to be a drain on the resources such as CPU time, power backup. This comparative analysis touches upon every parameter such as speed, block size, and key size etc. Application of Blowfish has a distinct advantage over DES, 3DES, and AES algorithms as could be seen from the narrative below.

Keywords: Security, AES, Blowfish, RSA.

I. INTRODUCTION

Cloud computing tends to be an interesting technology, with enormous business and marketing-related potentials. Clouds design the infrastructure better so that applications and related data can be accessed from anywhere. Enterprises pay to use the resources in cloud service providers for storage use and additional computing purposes. As a result, the cost of infrastructure in cloud environment is greatly reduced. It is said that one of the biggest drawbacks of cloud computing is Maximizing the allocated resources. Because the model is human As a consequence of the model's uniqueness, resource allocation is achieved with the aim of decreasing its relevant demands. Cloud Computing's resource management

approaches are widely supported in fixing and leveraging most of the significant physical resources.

Through a web browser or a lightweight desktop or mobile application, proponents exploit cloud-based applications whereas sensitive data storage software and user data are loaded on to servers at an isolated location. End users believe that cloud computing helps companies to get their apps up and run quicker, with better handling and less maintenance. In addition, the cloud system allows IT to accelerate the fine tuning of resources to bring together unpredictable and variable demand from enterprises.

Cloud computing depends on resource sharing to achieve consistency and quantity financing for a service, such as either a network electricity grid or the Internet. The wider thoughts of a single infrastructure and shared services are at the core of cloud computing. Most of the qualified equivalent data processing is performed using the Nephele agenda or the dynamic tool, provided by current IaaS clouds for both, job scheduling and implementation. More specific tasks of a processing job can be assigned to different kinds of virtual machines or servers that are often instantiated and triggered during execution of tasks. Researchers do research on a broader analysis of motivated processing jobs or on an IaaS cloud system, based on the processing job. Most of the existing systems, however, face limitations in terms of cost, complexity and increased organization based on the data.

Cloud computing provides companies to simplify their IT activities by handing over equipment and software control, plus associated support and maintenance obligations, to the cloud provider. Costs are reduced and converted from capital expenses to operating expenses, with the ability to grow capacity on demand. Yet there are risks that come with how you manage your infrastructure making such a significant change. It's important to have a robust plan in place to make the transition to ensure that you get the benefits.

The application we will implement will store the files in the cloud storage, based on the algorithm defined by the user. The Google drive, for example, will have a function to store the files in the cloud server and when a user needs them. It will allow the user to download and use it after checking the respective permissions.The file format can either be .txt, .pdf, .doc, etc. The uploading and retrieving rights will be common to all file types.

The main drawback of the Google drive is that they had not used any principles of security to encrypt and store the data in the cloud server. Just to retrieve or download the file from Google Drive they had mad and cross check with the access rights and the user details validation.The cryptographic algorithm is hard to change after the user has uploaded the data to the cloud storage. Because it takes us a huge amount of time to decrypt all the relevant user files and encrypt them with the new algorithm once again.

We should evaluate the accuracy and efficacy of the cryptographic technique used by the user after several days. Advanced Standard Encryption (AES), Blowfish Algorithm, and Reverse Blind Signature (RSA) are the algorithms used for the proposed work.

II. ANALYSIS OF VARIOUS CRYPTOGRAPHIC TECHNIQUES UPTO DATE

Many researchers have focused on finding the possible algorithms to provide 100 percent efficiency and accuracy to support the encryption and decryption process in the cloud server. The application developers had been paying attention to cryptographic techniques to solve the data security and data theft problem.

The existing applications were developed without encryption algorithms to provide high energy utilization and consumption of bandwidths in the cloud environment. Studies have also shown that cryptographic techniques bring better data security results. A few existing approaches are being developed in order to create a better security strategy and high energy usage.

A.AES Encryption and Decryption

Advanced Encryption Standard is a symmetric algorithm for the encryption of fixed data blocks (of 128 bits) at a time. The keys that were used to decode the text may be 128-, 192-, or 256-bit. The 256-bit key encrypts the data in 14 rounds, in 12 rounds the 192-bit key and in 10 rounds the 128-bit key. Each round consists of several steps in substitution, transposition, plaintext mixing, and more. Standards for AES encryption are the most widely used methods of encryption today, both for resting and transit data.

Next, some of the new standards were also set in encryption technique. One such approach was suggested by Abha Sachdev and Mohit Bhansali (2013) to boost cloud computing security using the AES algorithm [1]. The data and services in the cloud reside in massively scalable data centers and can be accessed anywhere.

Cloud computing has more advantages when it comes to running data-intensive applications. S.Delfin Prof., Sai. B Rachana, J.V Meghana, Lakshmi Kundana. Y, Sushmita Sharma, (2018) [2] Cloud computing allows for the use of Internet-based services by both large and small companies.

So they can minimize start-up costs, capital expenses, access apps only if need arises, use resources on a pay-as-you-use basis, and quickly lower or increase capacity. As the authors offer unparalleled skills and knowledge over the years, they discuss all the highly challenging topics such as data ownership, privacy protection, data mobility, service and service standards, bandwidth costs, data protection, and support.

Advanced Standard Encryption is one of the most common and mostly symmetric block cipher algorithms. This algorithm has a specific form in which subtle data can be encrypted and decrypted and is inserted into all hardware and software. It is very hard for the hackers to get the actual data as AES encrypts. There is no evidence to date to crack the algorithm. AES has the capacity to deal with 3 dissimilar key sizes such as AES 128, 192 and 256 bit. Each of its code has 128 bit.

Smitha Nisha Mendonca, (2018)[3] operated on demand-based computational infrastructure that has the power to reduce the cost of IT-based services development. It can provide various types of services over the internet. One of the cloud's significant resources is storage where users can store their data as needed.

It's a difficult problem for the user as all of the data is stored in some shared resource pool but this resource pool is spread in different parts of the world. An unauthorized user may be using the virtual machines to access that data. So, this is the dark side of storing cloud data. That insecurity creates a big user problem. The vulnerability creates a big user issue. Therefore data security is a big problem in cloud computing.

Shady Mohamed Soliman, Baher Magdy, Mohamed A. Abd El Ghany, (2017)[4] proposed advanced standard encryption algorithm for optimized designs in terms of output, area and power. The prototypes presented are appropriate for the AES-128 algorithm which is encrypted only. In one design both designs integrate pipeline and iterative architecture.

This is achieved by applying the concept of partial loop unrolling, where iterations and multi-stage pipelining are used to optimize area, performance and dynamic power consumption.

In this paper Parul Rajoriya, Nilesh Mohota, (2017)[5] offers an FPGA-based implementation of the Advanced Encryption Standard (AES) algorithm along with key image encryption. An efficient FPGA-based image encryption scheme is proposed using the AES algorithm built into the RC4 encryption standard. Use of the RC4 algorithm gives the encryption additional level of security.

Using Matlab the architecture transforms the original image into its hex values and then gives it to the proposed AES as input. Using the RC4 encryption algorithm the key input given to AES is further encrypted. Use AES decryption algorithm to decrypt the encrypted image. The encrypted key is decrypted using the RC4 decryption algorithm to give it to the AES decryption algorithm as its input.

The design uses an iterative looping approach with 128-bit block and key length, S-box implementing lookup table.

Prof S.Athinarayanan, S.Nivetha Priya, R.Supriya, (2011)[6] proposed two algorithms (a) Shamir's (k, n) threshold scheme and (b) AES (Advanced Encryption Standard) Shamir's (k, n) threshold scheme used to manage keys using K shares from n to reconstruct the key during decryption. AES Algorithm is used for device encryption and decryption.This Algorithm makes the system more reliable against hacking.

B.Blowfish Encryption and Decryption

Ms NehaKhatri–Valmik, Prof. V. K Kshirsagar, (2011)[7] is a 64-bit block cipher with a variable-length key that operated on blowfish. This identifies two distinct boxes: boxes S, box P and boxes 4 S[3]. The P box P is a one-dimensional field, with 18 32-bit values. The boxes contain variable values; these can be implemented in the code or created during each initialization process The S boxes S1, S2, S3, and S4 each contain 256 32-bit values.

The next writers focus on using Blowfish algorithm to introduce a banking system. Anupam Baruah, Prof.(Dr.)Lakshmi Prasad Saikia, (2011)[8] discusses some of the services, such as bill payment, transfer of funds, transfer, account statement viewing, etc. Users can easily access their e-banking account via internet using Wi-Fi or 3g/4 g connection via computers and smartphones. But safety of fund transaction is a very big issue.

There is a possibility that hackers can hack user account information at any time over the internet. Cryptography is a best method of encrypting data from outside Hackers. In this paper we use Blowfish algorithm to implement a banking system. This program will provide a secure web base application where users can access all information using a valid secret key only to be approved.

Pratap Chnadra Mandal, (2012)[9] introduces a fair comparison of four most common and commonly used symmetric key algorithms: DES, 3DES, AES and Blowfish. Based on these parameters a comparison was made: round block size, key size, and encryption / decryption time, CPU process time in the form of power consumption and throughput.These results show that blowfish is better than other algorithm.

S.Umadevi@Yasodhei, D.Nirmal Dev, K.Sakthivel, (2015)[10] the author created computing language or metaphor focused on computing resource usefulness and consumption. Cloud computing is architecturally based on the client-server. Cloud

computing means installing faraway storage departments and cloud networks allowing for consolidated garage records and online access to computer services or tools.

It is particularly vulnerable as 10 personal cloud server celebrities themselves have been hacked in the last three months due to many problems such as validity of documents, honesty, data hiding and availability. In this paper we implement a framework for the provision of protected information. We combine two Blowfish and AES algorithms to ensure security for passwords and cloud computing records.

Rashmi A. Gandhi, Dr. Atul M. Gosai, (2016)[11] with the rapid growth of the information and communication industries, data transfer, information communication, cloud data storage, sharing of valuable information across networks, raised the need for data security. With the advances in technology, data transmission is not limited only between computers / laptops that are now with the hand held devices like mobiles/tabs.

So it will also need attention along with data security, speed and power consumption. Cryptography is proven method for secure communication over networks. The rapid growth in digital data and its security raises concerns about the development of more advanced cryptographic techniques. There are algorithms for the various types of data such as text, image, audio, video, etc. Flow rates, speed, CPU time, Power Consumption and security are few parameters on which cryptographic algorithms are analyzed. The present paper analyzes some common symmetric cryptographic algorithms on the above parameters, such as DES, 3DES, AES and Blowfish. This paper offers a comparative analysis of the current techniques for cryptography. It also discusses an in-depth study of the Blowfish algorithm and the latest work done on it.

Shally Nagpal, Suneet Kumar, Suresh Chand Gupta, (2019)[12] plays a lively part to network security encryption. Many times, choosing the best encryption is a little bit confusing, as there are many methods of cryptography to secure the data during transmission. Blowfish is currently assumed to be insecure in many applications. So it turns out to be necessary to improve this technique by adding different safety rates so that it can be used in many reliable channels of communication.

Blowfish algorithm is updated in such a way that it is independent from the platform; however, the existing encryption schemes are limited to platform based proposal. This proposed algorithm changed to blowfish supports text, pictures, and media files.

C.RSA Encryption and Decryption

RSA implements a cryptosystem of public key, as well as digital signatures.

Saranya, Vinothini and Vasumathi, (2013)[13] consider the problem of intimidating challenges and solved an intimidating network security obstacle, allowing for safe but open exchange of encrypted communications between users and other parties (rsa.com, 2011).

In the early 20th century, a well-known electro-mechanical cipher machine, called the "enigma machine," was used to encrypt all confidential military and diplomatic information. Gowtham Ramakrishnan, (2019)[14] focused on developing an encryption crypto processor that will deal with key RSA algorithm generation, key distribution and encryption parts and also discusses the environment of verification required. The world of cryptography revolutionized with the advent of microprocessors in late 20th century. A cryptosystem is a chip system that includes algorithms of cryptography used for data encryption and

decryption. Such crypto processors are used in ATM communication systems and are highly portable.

Encryption and decryption are the essential processes that underlie every cryptosystem. There are many algorithms available for encryption and decryption; one such algorithm is known as the RSA (Rivest-Shamir-Adlean) Algorithm.

Mohit D.Singanjude, Prof. R.Dalvi, (2019)[15] provides the secure and fast way to send images using identity-based cryptography and visual cryptography. With Visual cryptography is used in this utility Identity Based Cryptography. In fully cryptographic identity the RSA cryptosystem is used to generate public and private key using Ancient Indian Mathematics for quick mathematical calculation. RSA is the algorithm which is fastest and most trendy. In multiplication phrases of field, vedic technique is so effective, compared to its current arithmetic implementation. The public / private key regeneration embraced to make the system safer from numerous attacks.

Pooja Devi, Naveen Tyagi and Parul Saharavat, (2018)[16] proposed algorithm that we use the subset sum problem hybrid combination and modified RSA cryptosystem. We are going to improve the security of the RSA algorithm in this work. Here we use three prime numbers instead of two, and add super-increasing sequences for the main generation process as well.

If Attacker wants to break proposed systems then the modulus must be factored into its primes, as well as the secret set A must be found. If modified RSA is broken in time x, which is based on a single module, and sub-set sum algorithm is broken in time y, then the time required to break this proposed algorithm is x*y. Therefore, as compared to the RSA algorithm, the security of our proposed system is increased.

The special protocol (RSA Handshake Database Protocol) was designed to controll this database development. Every gateway, which runs an Offline RSA-Key Generations process, is governed by specific issues and necessities. This stage is known as offline RSA-Key generations.

Sami A.Nagar and Dr. Saad Alshamma, (2012)[17] have proposed a new method for the exchange of key values between gates.

Aman Chadha, Sushmit Mallik, Ankit Chadha, Ravdeep Johar and M.Mani Roja, (2015)[18] suggest an RSA and Pseudo Noise (PN) video encryption algorithm for applications involving sensitive video information transfer. The algorithm is primarily formulated to work with Audio Video Interleaved (AVI) codec encoded files, although it can be easily ported to use with Moving Picture Experts Group (MPEG) encoded files. The source's audio and video components separately go through encryption layers to make some a cheap degree of security.

G.Sathish Kumar, K.Premalatha, N.Aravindhraj, M.Nivaashini, M.Karthiga, (2015)[19] the holder of the data encodes the data using its secret key. Afterwards the holder of the information encodes the secret key twice to frame an intermediate key. He / she will then give this encoded information to the server, and the middle of the road keys. The cloud unravels the middle of the road key in part and send the mostly decoded key and scrambled information to the planned beneficiary. The client will decrypt the somewhat decoded information sent by the cloud again and the client will get the key needed for decoding with the intention that the client will be able to decode it entirely.

Naveen N, K.Thippeswamy, (2019)[20] Approach of multi-layer encryption techniques in cloud computing thus enhancing security parameters with regard to sensitive data Thus, with layer ways Encryption techniques, data in the cloud server can be made more secure with better data protection. The resulting cloud side as well as the data owner benefit enhanced security.

According to this technique of encryption if the authorization of the data-owner is not granted then the users are restricted from accessing the data. The suggested methods are the advanced encryption standard (AES) symmetric encryption method and the Rivest-shamir Adleman (RSA) asymmetric encryption method.

Critical cloud applications will benefit from the aforementioned algorithm which claims to be simple and efficient. In the process of symmetric encryption, a single unique key should be exchanged amongst users who are bound for receiving messages, whereas in the process of asymmetric encryption, messages are encrypted and decrypted during contact using both private and private and public key. For the above two encryption algorithms responsible for the privacy and security of data related by way of the rest of the algorithms, the feasibility study is carried out later.

Parshotam and Rupinder Cheema and Aayush Gulati, (2019)[21] suggested a RSA change that would switch from the integer domain to the bit stuffing area to the first characteristic of SSL that could provide more secure communication. The emergence of bit stuffing would make it more difficult to get the correct entry to the message even after getting the private key admission. It will thus boost the security that is the necessary requirement for the design of secure communication cryptographic protocols.

Cloud computing is today a technological and social reality, while at the same time it is the emerging technology and security has become the main obstacle that hampers cloud environment deployment.

Dr. Rajamohan Parthasarathy, Ms. Haw Wai Yee, Mr. Seow Soon Loong, Dr. Leelavathi Rajamanickam, Ms. Preethy Ayyappan, (2019)[22] suggested a method for providing cloud data storage and security through the implementation of RSA algorithms using public key cryptosystems. The security services further describe include key generation, encryption, virtual environment decryption.

Manoj Agrawal, B. L. Pal, Rohit Maheshwari, (2015)[23] introduced RSAcryptosystem and enhancements to finding the decryption key value in its decryption method. Different methods have already been developed to reduce the decryption time such as CRT-RSA, Batch RSA, Re-balanced RSA, Multi Prime RSA, R-Prime RSA, etc. Our work proposed was carried out using MATLAB. We have tried the public key cryptosystem RSA for speed improvement in the decryption key generation time.

Also known as side-channel cryptanalysis done by this approach is called side-channel attacks. The attack that induced the information collected from the physical characteristics of cryptosystems to recover the secret key during run-time is known as timing attack.

Amuthan Arjunan, Praveena Narayanan, and Kaviarasan Ramu, (2015)[24] proposed a new technique called "Randomness Algorithm" and Optical Asymmetric Encryption Padding (OAEP) to increase the robustness of the RSA algorithm against timing attack by incorporating randomness in the process of decryption to make timing information unusable for the attacker..

III. ESTIMATION OF DATA SECURITY LEVEL

Most cloud enviroment inquiries also include data security concerns. Scientists are trying to deliver prominent cryptographic techniques to the cloud environment alongside efficient and high-level security. The algorithms we highlighted or used in this project are suitable for cloud environments and provide high-security encryption and decryption. With these powerful cryptographic algorithms, they find the stealing of information or data caught in the middle by the man pointless because they cannot convert them back to plaintext. The sub-section further elaborates on the current cryptographic techniques and their basic parameters.

A.Different Techniques Involved in Encryption and Decryption

Cloud computing based IT industry requires a permanent data security solution and its level of reliability. Implementing the best data security techniques is very necessary for each of the cloud service providers. Shady Mohamed Soliman, Baher Magdy, Mohamed A.Abd El Ghany, (2017)[25] proposed advanced standard encryption algorithms for optimized designs in terms of output, area and power.

The prototypes presented are appropriate for the AES-128 algorithm which is encrypted only. In one design both designs integrate pipeline and iterative architecture. This is achieved by applying the concept of partial loop unrolling, where iterations and multi-stage pipelining are used to optimize area, performance and dynamic power consumption.

Nishtha Mathura and Rajesh Bansode, (2017)[26] suggested an extension of a public-key cryptosystem to support an Advanced Encryption Standard and ECC Private Key Cryptosystem. Based on the AES main duration the past results were measured as 128 bit and no. This paper proposes a hybrid encryption scheme with iterations. The parameters to study will pay primary attention to the length of the important thing, no. Of the iterations to be implemented, and the form of aspect channel attack. For this work, the key duration was accelerated to 192 bit and the no. May be 12 of iterations taken.

Cloud storage services allow end users to store cloud data and enjoy high-quality on-demand cloud applications without the risk of data theft from data from their own software application.

Mohamed Ismail, Badamasi Yusuf, (2017) [27] addressed security threats records at the same time as cloud storage, robust authentication scheme and information encryption scheme introduce on this paper the use of Advanced Encryption Standard (AES) rules to encrypt user information content earlier than placing it in garage and authentication schemes for valid consumer verification and safety of unauthorized get entry to to all devices of system functionalities.

Cloud computing is known as product delivery rather than service. Cloud computing is about sharing the internet based infrastructure. Lots of consumers are putting their data in the cloud. Nevertheless, the fact that users still has physical possession of probably huge amount of sensitive data provides the credibility of the data.

S.Sweetlin Susilabai, D.S.Mahendran, S. John Peter, (2019)[28] attempted to improve the safety level of blowfish with the proposed Inter Bit Exchange and Merge (IBEM) data pattern which is fed into S-Boxes before application. Data pattern Inter bit Exchange and Merge (IBEM) helps the intruders not to easily find main mechanism what the user actually sends.

The results of all the exams performed leading to a common end that the protection of the Inter bit Exchange and Merge method provides records in a surprisingly secure manner as compared to the special algorithm of blowfish.

Ziaur Rahaman, Anjela Diana corraya, Mousumi Akter Sumi, and Ali Newaz Bahar, (2017)[29] focus on the AES Key Generation and Substitution Box process. It modifies the conventional approach to key generation and constructs the Advance Encryption Standard dynamic 3-Dimensional S-box. The proposed method indicates Matrix and S-box for 3-Dimensioanl Key Generation.

As proven this novel approach increases the amount of time it needs for encryption and decryption duration. The experimental result shows it also boosts the AES algorithm's electricity. The proposed method describes the theoretical assessment and the outcomes of the subsequent experiments.

B.The Essential Parameter of Encryption and Decryption

Several AES algorithms recently implemented in applications have been modified with the possible changes in critical parameters such as block size, key size, cipher size, etc. The available key sizes are 128, 192 and 256 bits, which are typically varied by the rounds. For instance AES-128 uses 9 main-round iterations, AES-192 uses 11, and AES-256 uses 13.The main four different sub-operations of AES are AddRoundKey, SubBytes, ShiftRows, and MixColumns.

Ahmed Tariq Sadiq, Faisal Hadi Faisal, (2017)[30] A modification of the AES algorithm is proposed in five proposals, the first modification is an extended plain text 4x4 for AES from 16 bytes to 64 bytes (8x8 array) this modified speed encryption, greater security and greater complexity, the second modification is an extended key by increasing the key length used from 176 bytes to 704 bytes For the encryption and decryption process because the change input state includes the key length, the change in key length makes the encryption more stable and more complicated, the third change is the shift row step by increment number of shifts in each row and the number of shifts depending on the part of the key, this change because the number of rows and columns in the state input is increased, the fourth change in the mixed column stage is changed. Modifications process based on how some parts of the key used in the development process improve the random sequence function within the algorithm.

Omer K.Jasim Mohammad, Safia Abbas, El-Sayed M.El-Horbaty and Abdel-Badeeh M.Salem, (2017)[31] presents an advanced encryption standard (AES) algorithm, considered to be the most eminent symmetrical encryption algorithm. The improvement focuses on the mixing technology between the fully S-Boxes built AES.

For encoding content, the quantity of rounds expanded, resulting in greater security for the framework. The underlying key was created from the square at Polybius. With the expansion of the number of rounds, more computational investment will be required and the framework will be severely breached.

We are reasoning it can create the multi-faceted quality of finding the first content. It gives high protection and high confidentiality of details. Efficient implementation of cipher blocks is very important with a good understanding of the cryptographic algorithm, to achieve high efficiency and accuracy. N' block cipher numbers including Advance Encryption Standard have been implemented in various platforms and application.

Jayant P.Bhoge, Dr. Prashant N.Chatur, (2017)[32] presents the implementation of the Advance Encryption Standard algorithm and explains the effect of Avalanche with the aid of the test results. To this end we use the Xilinx ISE 9.1i platform in the development of Algorithms and the ModelSim SE 6.3f framework for validation and calculation of results.

IV. CRYPTOGRAPHIC TECHNIQUES FOR CLOUD SERVER

Because of the high energy utilization and very slow processing, most cryptographic algorithms are not suitable for cloud servers. Key points to keep in mind in any environment are performance, encryption strength and key exchange. Data security in the cloud is enhanced as end users encrypt data before uploading to the cloud server and store all information related to security stored in cloud application server thus removing the possibilities of system administrator attacks. The use of asymmetric encryption for cloud environments such as RSA 2048 is a better choice where performance is not an issue. This mechanism gives cloud environment a more secure key exchange scheme. Where performance is required, use symmetric encryption, and then use the same mechanism for key exchange in cloud environment.

A.Suitable Encryption techniques for Cloud Server

RSA 2048 is one of the appropriate cloud server or cloud storage encryption techniques, and belongs to the asymmetric encryption family. It has 617 decimal digits, the highest of all RSA numbers. D.Palanivel Rajan, Dr. S.John Alexis, (2017) [33] Cloud Computing moves computer applications and databases to large data centers where data and resources management can take place.

Nonetheless, this specific feature introduces several new, challenging security situations that have not been well understood. Security is about safeguarding records from danger and vulnerability. There are so many risks and vulnerabilities that need to be addressed.

There are still some challenges to resolve among which the issues of security and trust are crucial. The various types of encryption algorithms are discussed in detail in this paper and the performance of these algorithms is evaluated to analyze the cloud platform's best algorithm. This discusses the different open research questions and challenges presented in the cloud platform

Cloud Computing addresses many traditional computing issues, including managing peak loads, downloading updates to applications, and using insufficient computing cycles. However, the new technology also created new challenges such as data security, data ownership and data storage of trans-codes.

Sanjoli Singla and Jasmeet Singh, (2013)[34] used the EAP-CHAP Rijndael Encryption Algorithm. This method brings about many new challenges, which have not been well understood any more. However, security and privacy issues are amongst the pinnacle concerns that stand in the way of wider cloud adoption. The main topic in cloud computing is to provide the security to quit person to protect files or facts from unauthorized consumers. Security is the main goal of any era that prevents unauthorized intruder from entering your file or cloud statistics. We have developed a proposed layout and structure to help encrypt and decrypt the person-faced text.

B.Accuracy of Cryptographic Techniques in Cloud

Considered as a model for monitoring information security rules, confidentiality, integrity and availability are. The main issue is treated as being confidentiality. They deal with unauthorized or unauthenticated data access. This can be solved by cryptography Prof. (Ms.) Kimaya Ambekar, Prof. (Dr.) R.Kamatchi, (2018)[35] uses a cloud security model and tries to test the effect of different types of models. The inclusive results of various algorithms and multi-level encryption algorithms are analyzed on the basis of different parameters for the performance evaluation.

Seungmin Kang, Bharadwaj Veeravalli, and Khin Mi Mi Aung (2018)[36] designed and implemented an ESPRESSO (Encryption as a Cloud Storage Systems Service) encryption provider to secure user data by using advanced encryption algorithms. ESPRESSO's bendy interface and stand-alone belongings allow cloud storage providers to easily combine it with heavy amendment and implementation in their infrastructures. ESPRESSO has been incorporated into two cloud storage systems which are open source: OpenStack / Swift and Nimbus / Cumulus.

Murtala Aminu Baba, Abdulrahman Yusuf, Aminu Ahmad, (2014)[37] with the boom of unauthorized access to confidential cloud statistics, this paper provides encryption strategies that provide robust assault security through Transparent Data Encryption (TDE). To secure the confidentiality of the cloud database, TDE is used to encrypt and defend information in a transparent manner, on toughness, in transit and on backup media. TDE is reliable, clean and provides the columns, tables and desk space with excessive security levels for documents that require protection. This paper explores the efficiency of encryption algorithms (AES128, AES192, AES256, and 3DES168) with respect to CPU time, time of execution, and time of transfer. AES128 is expected to have a higher overall performance than different encryption algorithms.

Table 1, shows comparison of various cryptographic algorithms based on different factors.

TABLE1: Comparison of different cryptographic algorithms

Algorithm	Key Size	Speed	Dependency	Security
AES	128, 192, 256 bits	Fast	Yes	Secure
Blowfish	32-448 bits	Fast	No	Secure but less verified
RSA	1024 bits and above	Fast	Yes	Secure

V. RESEARCH GAP

Because of the performance issue, such as the slowness of 3 Key Triple Data Encryption Standard (DES) algorithms, use was stopped and Advanced Standard Encryption (AES) photographed in 1998. The Advanced Standard Encryption (AES) has 3 separate bit keys, depending on block rounds. The 128-bit AES algorithm was the first to arrive at the advanced Standard Encryption (AES). Each key differs with the number of cycles or round number it takes to process and generate the keys and each cycle or round takes one block which is 16 bytes long.

The Advanced Standard Encryption (AES) padding standard has different phase and different encryption types, depending on the changes brought in the cypher. Each encryption process round is composed of four separate subprocesses. The parameters of the S-box have been modified to overcome performance drawback in cloud environment.

The Blowfish Algorithm is a 64-bit block symmetric block cipher, and its key length can vary from 32 bits to 448 bits. Blowfish is fast, open source and an alternative to the existing algorithms for encryption. Blowfish Algorithm is more vulnerable to birthday attacks because the keys are generated using a 64-bit block cipher.

RSA algorithm is an asymmetric cryptographic algorithm that has two distinct keys and is both public and private. It is therefore sometimes called public key cryptography, and can be exchanged with anyone. Without the private key, we cannot decipher the encrypted text into plain text. It's based on the very difficulty of finding the factors of a large number of composites. Because the integers number which are used are prime numbers and it is called as prime factorization.

While a lot of cryptographic algorithms arrived in a short span of time, we had tailored a few parameters, such as cipher mode, block size, salt size, iv key generation process, etc., and used them in this proposed project.

VI. CONCLUSION

The main contributions are as follows

- 1) To improve the proposed Advanced Standard Encryption (AES) encryption method.
- 2) To increase the size of the AES algorithm's secret key so as to achieve a high level of safety. The attacker in turn will not be able to find out the size of the secret key and will not be able to hack the data in the network layer.
- 3) Changing the AES algorithm padding to no padding to change the predefined AES block size.
- To improve the performance of cryptographic algorithm in cloud environments, use Rivest-Shamir-Adleman (RSA 2048) Algorithm.

5) Reducing the computational cost and complexity involved in cryptographic use of symmetric algorithms in cloud applications at very low load locations.

6) Lastly, ensuring a high level of cloud storage protection with an effective encryption technique via AES 256-Bit in cloud computing environments.

REFERENCES

[1]. Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security Using AES Algorithm", International Journal of Computer Applications, Vol. 67 , No 9, April 2013.

[2]. Prof.S.Delfin1, Rachana Sai.B2, Meghana J.V3, Kundana Lakshmi.Y4, Sushmita Sharma5," CLOUD DATA SECURITY USING AES Data Security in Cloud using AES Algorithm", International Research Journal of Engineering and Technology(IRJET), Volume: 05 Issue: 10| Oct2018, Page 1189.

[3]. Smitha Nisha Mendonca , "Data Security in Cloud using AES", INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY,VOLUME 07, ISSUE 01 (JANUARY 2018).

[4]. Shady Mohamed HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212"Soliman HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" ; Baher HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094"Magdy HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" ; Mohamed A. HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500"Abd HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" El HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500"Ghany HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" HYPERLINK "https://ieeexplore.ieee.org/author/37399998500" ," Efficient implementation of the AES algorithm for security applications ",Publisher: IEEE.

[5]. P Rajoriya, N Mohota ," REVIEW ON FPGA IMPLEMENTATION OF IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM ALONG WITH KEY ENCRYPTION", techchronicle.in.

[6]. S Athinarayanan, SN Priya, R Supriya,"Secure Data with Key Managers by Using Shamir Scheme and AES Algorithm", pdfs.semanticscholar.org.

[7]. Neha Khatri –Valmik," BLOWFISH ALGORITHM", International Journal Of Engineering Sciences & Management.

[8]. Anupam Baruah1, Prof. (Dr.)Lakshmi Prasad Saikia, "Biometric System Using Cryptography:A Survey", IJCSMC, Vol. 4, Issue. 9,September 2015, pg.101 –104.

[9]. Pratap Chnadra Mandal," VALUATION OF PERFORMANCE OF THE SYMMETRIC KEY ALGORITHMS: DES, 3DES ,AES AND BLOWFISH", Page | 196Volume 2, Issue 9,September2012,International Journal of Advanced Research in Computer Science and Software Engineering.

[10]. S.UMADEVI@YASODHEI, D.NIRMAL DEV, K.SAKTHIVEL," Triple Encryption Methodon Passwordfor Secured Cloud Data Storage in Mobile", IJCSMC, Vol. 4, Issue. 3, March 2015, pg.265–270.

[11]. Rashmi A. Gandhi, Atul M. Gosai," A Study onCurrent Scenarioof Audio Encryption", International Journal of Computer Applications (0975 –8887)Volume 116 –No. 7, April 2015.

[12]. Shally Nagpal, Suneet Kumar, Suresh Chand Gupta,"A New Method for Modifying Blowfish Algorithm for IoT", International Journal of Innovative Technology and Exploring Engineering (IJITEE),ISSN: 2278-3075, Volume-8, Issue-9S, July 2019.

[13]. Saranya, Vinothini, Vasumathi, "Securing Sensitive Information Files Based on Session Keys ... HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL" HYPERLINK "https://www.google.com/url?sa=t HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"rct=j HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-

BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"q= HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"esrc=s HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"source=web HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"cd=2 HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468 HYPERLINK

"https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL" HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"", HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL" HYPERLINK "https://www.google.com/url?sa=t HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"rct=j HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"q= HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"esrc=s HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Fin

dex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"source=web HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"cd=2 HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468 HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"& HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL" HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL" HYPERLINK "https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi2j6K8xN_mAhXn4zgGHRW8AD0QFjABegQIBhAG&url=http%3A%2F%2Fwww.indjst.org%2Findex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"dex.php%2Findjst%2Farticle%2Fview%2F141468&usg=AOvVaw17XZXc7lBDIt7WjwF-BwqL"

A study on RSA algorithm for cryptography, ... 2013; 2(6):126–39.

[14]. Gowtham HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943" HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22 HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"& HYPERLINK

"https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"start=0 HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"& HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"context=3899943" HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943" HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943" HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22 HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"& HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"start=0 HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"& HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"context=3899943" HYPERLINK "https://scholarworks.rit.edu/do/search/?q=author_lname%3A%22Ramakrishnan%22%20author_fname%3A%22Gowtham%22&start=0&context=3899943"Ramakrishnan, "Design and Verification of an RSA Encryption Core", THESES > 10067.

[15]. Mohit D. Singanjude Prof. R. Dalvi," Literature Survey: Secure transmitting of data using RSA public key implemented with Vedic method",10.7753/IJCATR0510.1009.

[16]. Pooja HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" Devi, HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=%20Naveen%20Tyagi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi"Naveen HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=%20Naveen%20Tyagi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi"Tyagi HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=%20Naveen%20Tyagi" HYPERLINK "http://ijsrcseit.com/search_result.php?search=Pooja%20Devi", Parul Saharavat ," Three Prime RSA Algorithm Using Randomly Generated Prime Sequence Cryptosystem", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN : 2456-3307.

[17]. Sami A Nagar, Saad HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma" HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma" HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma" HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma" HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma" HYPERLINK "https://www.researchgate.net/scientific-contributions/2045838503_Saad_Alshamma"Alshamma, "High speed implementation of RSA algorithm with modified keys exchange", DOI: 10.1109/SETIT.2012.6481987,Conference: Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 .

[18].Aman HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A"query=Chadha%2C+A" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A" Chadha, Sushmit HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S"query=Mallik%2C+S" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S"query=Mallik%2C+S" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Mallik%2C+S"Mallik, Ankit HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A"query=Chadha%2C+A" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Chadha%2C+A" Chadha, Ravdeep HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R"query=Johar%2C+R" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R"query=Johar%2C+R" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Johar%2C+R"Johar, M.

Mani HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Roja%2C+M+M" HYPERLINK "https://arxiv.org/search/cs?searchtype=author HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Roja%2C+M+M"& HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Roja%2C+M+M"query=Roja%2C+M+M" HYPERLINK "https://arxiv.org/search/cs?searchtype=author&query=Roja%2C+M+M"Roja,"Dual-Layer Video Encryption using RSA Algorithm", (Submitted on 14 Sep 2015),Cornell university.

[19]. G.Sathish Kumar,K.Premalatha,N.Aravindhraj, M.Nivaashini, "Secured Cryptosystem Using Blowfish and RSA Algorithm for The Data in Public Cloud",International Journal of Recent Technology and Engineering (IJRTE),3878, Volume,7.

[20]. Naveen N, K.Thippeswamy,"Security andPrivacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments",International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075, Volume-8 Issue-8 June, 2019.

[21]. Parshotam, Rupinder Cheema, Aayush Gula," Improving the Secure Socket Layer by Modifying the RSA Algorithm",International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.3, June 2012.

[22]. Dr.Rajamohan Parthasarathy, Ms.Haw Wai Yee, Mr.Seow Soon Loong, Dr.Leelavathi Rajamanickam, ,Ms. Preethy Ayyappan, "Implementation of RSA Algorithm to Secure Data in Cloud Computing", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4.

[23]. Manoj Agrawal, B. L. Pal and Rohit Maheshwari,"Improvement Over Public Key Cryptosystem RSA by Implementing New Decryption Key Generation Algorithm", International Journal of Engineering and Management Research, Page:300-304.

[24]. Amuthan Arjunan, Praveena Narayanan, and Kaviarasan Ramu," Securing RSA Algorithm against Timing Attack", The International Arab Journal of Information Technology, Vol. 13, No. 4, July 2016 471

[25]. Shady Mohamed HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212"HYPERLINK "https://ieeexplore.ieee.org/author/37085996212"SolimanHYPERLINK "https://ieeexplore.ieee.org/author/37085996212" HYPERLINK "https://ieeexplore.ieee.org/author/37085996212"HYPERLINK "https://ieeexplore.ieee.org/author/37085996212" ; BaherHYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094"HYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094"HYPERLINK "https://ieeexplore.ieee.org/author/37085993094"MagdyHYPERLINK "https://ieeexplore.ieee.org/author/37085993094" HYPERLINK "https://ieeexplore.ieee.org/author/37085993094"HYPERLINK

"https://ieeexplore.ieee.org/author/37085993094" ; Mohamed A. Abd El Ghany , "Efficient implementation of the AES algorithm for security applications ",Publisher: IEEE.

[26]. Nishtha Mathura, Rajesh Bansode," An Improved AES Cryptosystem Based Genetic Method on Secure AES", (IJAERS) [Vol-4, Issue-3, Mar- 2017].

[27].Mohamed Ismail,BadamasiHYPERLINK "https://www.researchgate.net/profile/Badamasi_Yusuf" HYPERLINK "https://www.researchgate.net/profile/Badamasi_Yusuf"HYPERLINK "https://www.researchgate.net/profile/Badamasi_Yusuf" Yusuf,," ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH ADVANCED ENCRYPTION STANDARD (AES) AND AUTHENTICATION SCHEME (AS)", DOI: 10.24924/ijise/2016.11/v4.iss1/18.39

[28]. Sweetlin Susilabai, D.S. Mahendran, S. John Peter," Interbit Exchange and Merge (IBEM) Pattern of Blowfish AlgorithmS.", International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878, Volume-7 Issue-5S2, January201.

[29]. ZiaurHYPERLINK "https://www.researchgate.net/profile/Ziaur_Rahman19" HYPERLINK "https://www.researchgate.net/profile/Ziaur_Rahman19"HYPERLINK "https://www.researchgate.net/profile/Ziaur_Rahman19" Rahman, AnjelaHYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya" HYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya"HYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya" Diana HYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya" HYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya"HYPERLINK "https://www.researchgate.net/profile/Anjela_Corraya"Corraya, MousumiHYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"AkterHYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi" HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"HYPERLINK "https://www.researchgate.net/profile/Mousumi_Sumi"Sumi," A Novel Structure of Advance Encryption Standard with 3-Dimensional Dynamic S-box and Key Generation Matrix", International Journal of Advanced Computer Science and Applications 8(2) · February 201.DOI:10.14569/IJACSA.2017.08024.

[30]. Ahmed Tariq Sadiq1, Faisal Hadi Faisal," Data Encryption Using Modified AES for Android Mobile", Journal of Advanced Computer Science and Technology Research, Vol.7 No.3, September2017, 81-85.

[31]. D.I. George Amalarethinam1and H.M. Leena, "A Comparative Study on various Symmetric KeyAlgorithms for enhancing Data Security in CloudEnvironment", International Journal of Pure and Applied Mathematics, Volume 118 No. 6 2018, 85-94.

[32] Abdullah Al- Mamun1, Shawon S. M. Rahman, Tanvir Ahmed Shaon1 and Md Alam Hossain1," SECURITY ANALYSIS OF AES AND ENHANCING ITS SECURITY BY MODIFYING S-BOX WITH AN ADDITIONAL BYTE", International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.2, March 2017DOI: 10.5121/ijcnc.2017.920669.

[33]. D, Palanivel Rajan, Dr. S. John Alexis" Comparative Study on Data Encryption Algorithms in Cloud Platform", International Journal of Engineering Research & Technology,-pdfs.semanticscholar.org.

[34]. Sanjoli Singla, Jasmeet Singh," Cloud Data Security using Authentication and Encryption Technique",
ISSN : 2454-9150 Vol-01, Issue 09, Dec 2015. INJRV01I09001 www.ijream.org © 2015, IJREAM All Rights Reserved. 4 ... Communications (IJCNC) Vol.5, No.2, March 2013. Global journal of science and technology.Vol-13,No 3-B(2013).

[35]. Kimaya Ambekar,R. Kamatchi," Enhanced User Authentication Model in Cloud Computing Security", The International Symposium on Intelligent Systems Technologies and Applications , ISTA 2016: Intelligent Systems Technologies and Applications 2016,Page no: 327-338.

[36].BharadwajVeeravalli, Khin Mi MiAung," Dynamic scheduling strategy with efficient node availability prediction for handling divisible loads in multi-cloud systems", Journal of Parallel and Distributed HYPERLINK "https://www.sciencedirect.com/science/journal/07437315" HYPERLINK "https://www.sciencedirect.com/science/journal/07437315"HYPERLINK "https://www.sciencedirect.com/science/journal/07437315"Computing,VolumeHYPERLINK "https://www.sciencedirect.com/science/journal/07437315/113/supp/C" HYPERLINK "https://www.sciencedirect.com/science/journal/07437315/113/supp/C"HYPERLINK "https://www.sciencedirect.com/science/journal/07437315/113/supp/C" 113, March 2018, Pages 1-16.

[37]. Murtala Aminu Baba, Abdulrahman Yusuf, Aminu Ahmad," Performance Analysis of the Encryption Algorithms as Solution to Cloud Database Security", International Journal of Computer Applications (0975 –8887)Volume 99 –No.14, August 2014.