iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IX **Month of publication:** September 2017

DOI: http://doi.org/10.22214/ijraset.2017.9101

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

Surveillance in Cloud Data Using Hybrid Algorithms

Shaik. Shahanaj Begam[1], N. Neelima[2],
[1, 2] *Department of computer science and technology, Velagapudi Ramakrishna Siddhartha Engineering College*

Abstract*: Cloud computing is the mechanism to provide on demand service access and providing computing resources on the internet. To manage this vast quantity of information it's highly suggested to confirm its security, control its access. The cloud storage space is centralized but cloud access will be done remotely. Then it's far possible there can be security violation or any intruder attacks while storing the information inside the cloud. So security of cloud is really vital. Now, this paper introduces a latest security approach use the hybrid of two algorithms, AES and Blowfish which was implemented in a cloud environment. Also compare, analyze RSA along with Blowfish and AES along with Blowfish for finding an efficient encryption algorithm which takes much fewer time.

***Keywords*: Cloud computing, Security, AES, RSA, Blowfish algorithm**

I. INTRODUCTION

Cloud Computing is being viewed as an emerging field in the IT trade because it offers scalable "on demand service" to the clients over the net. Cloud Computing objective is to provide the resources to the clients as per their order only. Cloud permits client to pay as per their requirement and need not pay for the unused required resources. It is an efficient way to use or share resources because it offers business to several people remotely above the Internet. Thus, client and vendor need not come face to face to make the deal and each can be served for their purposes remotely over the net via Cloud Computing. There were many companies has their own clouds such as Google, Amazon, Microsoft, IBM, Oracle and so on, to help the people to get assets of cloud services.

A. Deployment Models

There are distinctive types of deployment models in cloud computing. These are

1) *Public Cloud:* Public cloud is a cloud computing deployment model in which service provider makes sources, which include applications and storage space, above the net. It provides benefits to the users for free or offered for the pay-per-usage model. It is a third-party provider provides the cloud assets i.e., sold on demand, on the basis of hours or days. Consumers only pay for storage, bandwidth, CPU cycles which they consume. Examples of public clouds include Amazon EC2, IBM's Blue Cloud, and Jelastic Cloud.
2) *Private Cloud*: Private cloud is a computing infrastructure which is associated with specific company and not shared with different companies. These clouds are greater costly and more protected while compare with public cloud. Examples of these cloud include Amazon VPC, VMware Cloud Infrastructure Suite.
   Private cloud is two types:
   a) *On-premise private cloud:* On-premise private cloud evolves enterprise storage from traditional, purchased hardware, software, and assets into a pay-as-you-go, absolutely managed, on-website online service with expected, natural running prices. It get rid of the requirement to make investments capital into organization storage infrastructure and offers cloud-scale capability and overall performance with enterprise SAN(Storage Area Network) and NAS(Network Attached Storage) functionality at subscription-based pricing.
   b) *Externally hosted private clouds:* These clouds are completely used by single enterprise, however, hosted by using a third-party that specialize in cloud infrastructure. On-premise private cloud is expensive than Externally hosted private clouds.

3) *Hybrid Cloud:* Hybrid cloud uses a blend of public, private, third-party, on-premises cloud services between two platforms. It offers capability to sustain the cloud as retrieval of data is easy within the cloud. By way of permitting workloads to move between private and public clouds as computing requirements and prices modification and it also commerce with greater flexibility. Examples of Hybrid Cloud include Windows Azure, VMware vCloud.

4) Community Cloud: It distributes infrastructure between various companies from a unique community with frequent issues (security, compliance, etc.), whether or not managed inside or by a third-party, and either hosted internally or outwardly. The prices are unfold over less consumers than a public cloud (however extra than a private cloud), just only some of the charge savings capacity of cloud computing.

Community Cloud has two scenarios:

a) On-site community cloud scenario: It is inclusive of a web server with susceptible information, can be situated at every of the member sites where cloud assets are provided. It applies to community clouds enforced on the location of the consumers composing a community cloud.

b) Outsourced community cloud scenario: In an outsourced community cloud scheme, there's one security parameter applied with the aid of a community cloud supplier and other security parameter enforced by every cloud customer. The cloud provider security perimeter is connected to the security perimeters of more than single cloud customers in a factor to multi-point configuration the usage of depended on internet connections. It applies to community clouds wherein the server aspect is outsourced to a web hosting company. Example for Community cloud is Microsoft Government Community Cloud.

B. Service Models of Cloud Computing

There are 3 service models in cloud computing:

1) Software as a Service (SaaS): Saas is one of the service model during a third-party supplier hosts applications along with available to consumers above the net. It eliminates the necessity for companies to build in and run apps on their private computer systems or in their own data centers. Then it gets rid of the price of hardware acquisition, provisioning and maintenance, additionally as software licensing, installation and support[1]. Examples of SaaS include Email, Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM) etc.

2) Platform as a Service (PaaS): Platform as a Service (Paas) is a cloud computing version which gives a platform permitting clients to develop, run and manage programs without the complexity of building and keeping the infrastructure. PaaS vendors can pay for that access on a usage basis. Some PaaS vendors can take money for monthly basis to access the platform and the applications hosted on it. PaaS offerings afford application design, development, testing, deployment and hosting. Examples of PaaS include Google App Engine, Amazon Web Services (AWS), and Microsoft Azure etc.

3) Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) offers virtualized computing sources above the web. It is a third-party supplier host's software, hardware, storage, servers and different infrastructure elements on behalf of its consumers. IaaS vendors additionally host consumer applications and handle responsibilities including system maintenance and backup. Other services it consists of the automation of administrative responsibilities and desktop virtualization. IaaS users pay on according to per-user basis by the day, week or month. Examples of IaaS include Amazon Web Services (AWS), IBM Smart Cloud Enterprise etc.

II. RELATED WORK

A. Jasleen Kaur, Sushil Garg [7]

"Security in Cloud Computing uses Hybrid of Algorithms", proposed a hybrid algorithms that have been enforced could be a grouping of 2 algorithms broadly used asymmetric and symmetric algorithms i.e, RSA as Digital Signature and Blowfish Algorithm. RSA as Digital Signature objective to offering validation and non-repudiation of the message and Blowfish algorithm is a fast secret key cryptography and it's used for decryption and encryption purpose. The performance of this algorithm is complicated and is hard to be interpret by any intruder. Once the file is signed and encrypted the usage of the hybrid algorithm, two copies of the digital signature are created out of which one is stored locally and other is upload in the cloud along with the encrypted message. For decryption, the document will be decrypted usage of Blowfish and then digital signatures are matched with the copy of digital signature stored into cloud.

B. Sanjoli and Jasmeet [5]

"Cloud data security using authentication and encryption technique", advise to combine of 2 cryptographical algorithms, Rijndael Encryption Algorithm and EAP-CHAP. EAP is employed to offer verification access to the cloud environment. CHAP, is a technique of EAP, is enforced for verification reason. The complete methodology involves few steps. In first step, Cloud Service Provider receives an verification request from the user. In next step, CSP delivers acknowledgment after checking the consumer identification use of EAP-CHAP. In next step, the consumer is verified, the customer encrypts the data using Rijndael Encryption

Algorithm and uploads the cipher text data directly to the server of CSP. In this paper, client side protection has been focused and encryption in the hands of the user for providing better security.

C. Shirole and Sanjay [4]

"Data Confidentiality in Cloud Computing with Blowfish Algorithm", endorse a system that creates usage of cryptography method to offer dependable and quick manner to protected data for resolve safety measures challenges. Scheduler performs cryptography on plain text into cipher text followed by uploading of ciphered text within the cloud. When the data to be retrieve from the cloud, it is acquired in plain text format and saved within the system, this safeguard the data internally. Hence, this builds a association of collaboration between operator and service provider. This model uses OTP(One-Time Password) for verification and Blowfish algorithm for encryption.

D. Garima and Naveen [3]

"Triple Security of Data in Cloud Computing", state that it uses steganography and grouping of two cryptographic algorithms. This paper proposes a Steganography and grouping of two cryptographic algorithms DSA and AES. DSA is employed for authentication, AES is employed for encrypting the data and Steganography is employed for further encryption. The functioning involves the signing of the data within the first step. The signature is generated by initial applying a hash function on data and gives the compact type of data that is called message digest. The message digest has then signed the usage of the sender's private key. Once the message is signed, the text is ciphered along with the signature using AES. After encryption, Steganography secretes message along with every media which does lure the attention of an intruder and therefore the information is protected. This paper concludes that the time complexity of the entire mechanism is high since it is one by one process.

E. Parsi and Sudha [2]

"Data Security in Cloud Computing uses RSA Algorithm", state that to offer data safekeeping in a cloud environment. In the proposed system, RSA could be a public key cryptography and it's far used for both decryption and encryption of data and this procedure includes encryption of data and then uploading in the cloud. For decryption the requisite data is downloaded from the cloud, cloud provider authenticated the client after which the information is decrypted. The functioning of RSA abides by 2 keys: a public key and private key. The private key is only available to the authorized data owner while the public key is distributed and shared with others.

III. PROPOSED WORK

The hybrid algorithm which has been implemented is a grouping of two extensively used symmetric algorithms i.e., AES and Blowfish algorithm. AES is used for authentication and verification purpose and Blowfish is used for encryption and security purpose.

A. AES

Advanced Encryption Standard (AES) is symmetric encryption-algorithm which is well designed hardware and software program with a various block lengths of key sizes like 128,192,256 bit. While AES performs different cycles for different keysizes. For 128 bit it uses ten cycles, for 192 bit it uses twelve cycles, for 256 bit it uses fourteen cycles. For every of those rounds it uses different 128 bit round keys, that calculate in the pre-round transformation.

1)Process of AES:

a) *Sub Bytes:* It has 16 input bytes which are substituted by searching up a fixed table. The outcome is in 4X4 matrix form.
b) *Shift Rows:* It is a transposition step, rows of the states are shifted.
c) *Mix Columns:* By using a mathematical function each column of 4 bytes is transformed. This operation takes as input the 4 bytes of 1 column and outputs 4 completely new bytes, which replace the first column.
d) *Add Round Key:* The sixteen bytes of the matrix as 128 bits and XORed to the 128 bits of round key. It is the finishing round then the end result is within the cipher text.

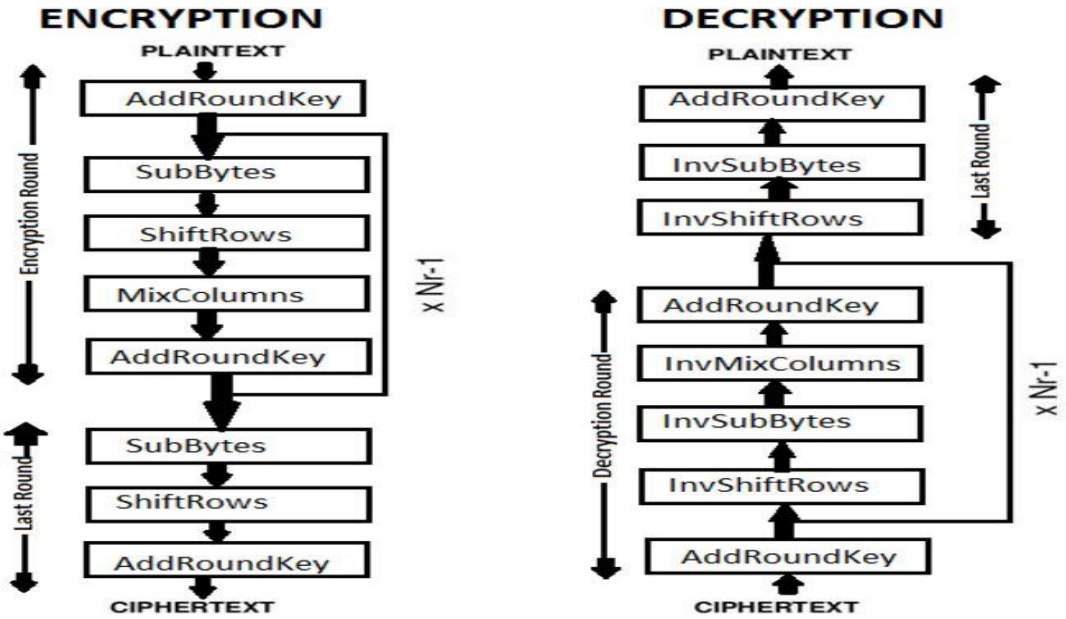


Fig. 1 AES Algorithm

AES implements following procedure for encryption or decryption:
AES algorithm uses round key function, in order to generate round keys we use Rijndael's algorithm.
The plaintext is transformed into four x four matrix.
Each byte of every round is mixed with round key by the help of bitwise xor.
Rounds will be performed until 10 rounds, In the previous nine rounds, it calculates 4 steps.
In each phase byte substitution is done and s-box is performed for encryption and with inverse s-box decryption is performed depends on the previous result.
In shift row phase, 1st row of matrix is remains same, in the 2nd row it shifts 1 bit from the left, in 3rd row it shifts 2bits from left and so on. In decryption phase it is quite opposite to encryption i.e., to the rows are shifted to right.
In mix columns phase every byte replaces 4bytes in the column
In add round key phase each byte of every round is mixed with round key by the help of bitwise xor.
In final phase only 3 steps are performed, blends columns phase is not performed in the final round.

B. Blowfish

Blowfish is the symmetric-key block cipher and in a massive variety of cryptographic and encryption outcomes. Blowfish is a block length of 64-bit and a changeable key size which vary from 32 bits to 448 bit. The process have 16 rounds Feistel cryptographic and big key-dependent S-boxes are used for encryption/decryption. The algorithm uses 2 sub key arrays are 18th entry P-array and four 256-entry S-boxes. The S-boxes take 8-bit input and give 32-bit output. In each round, an entry from P-array is taken, and following the last round, each semi of the data block is XOR with one of the 2 last unused P-entries.

1) *Process of Blowfish:* The encrypted data of 64bit input is marked with p, whereas the P-array is marked with a Xi (where i is the iteration).

The p is the 64bit data element taken as input.
Divide p into two 32bit equal halves i.e., pL, pR.
Then, for i = 1 to 16.
pL = pL XOR Xi pR = F(pL) XOR pR
Swap pL and pR
After the sixteenth round, swap pL and pR again to undo the previous swap.
Then, pR = pR XOR X17 and pL = pL XOR X18.
Finally, recombine pL and pR to get the cipher text.

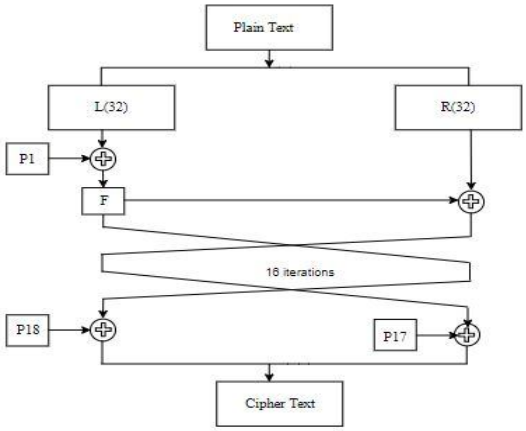


Fig. 2 Blowfish Algorithm

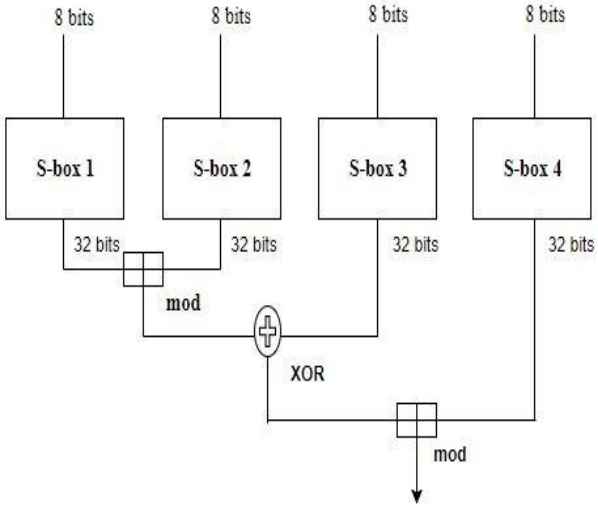


Fig. 3 Function of S-Box

C. Working of Hybrid Algorithms

The working algorithm consists of a grouping of 2 algorithms: AES and Blowfish algorithm. AES is employed for authentication and verification purpose and Blowfish is employed for cryptography and security purpose for documents.

1)Working of AES:

Data Owner is registered to upload or download the files.
Data Owner enters the login details to upload or download the documents.
When the Data Owner enters his password a hidden key is generated.
The generated key is mailed to the Data Owner's mail.
The Data Owner enter the hidden key and click on submit.
When the authentication details are matched the Data Owner can redirect to their home page.
Then the Data Owner can upload, view, edit/delete the documents.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

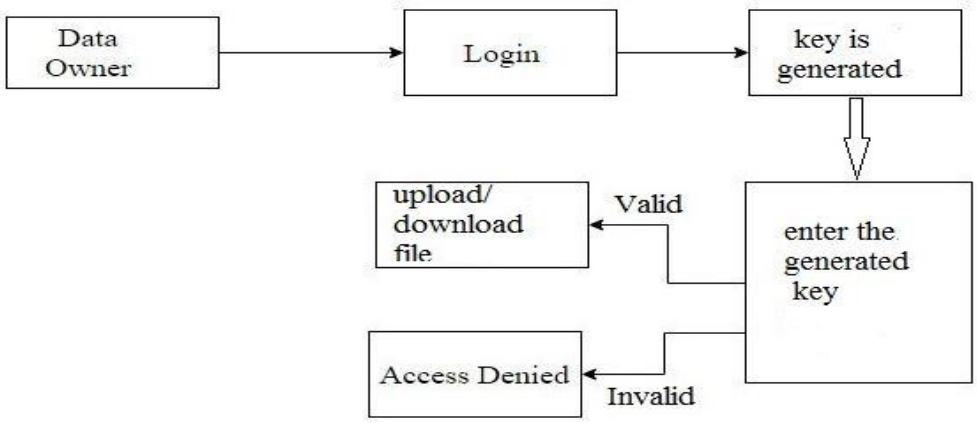


Fig. 4 Working of AES

2)Working of Blowfish: Before applying blowfish algorithm, data owner authentication is mandatory.
When Data Owner is authenticated, then the data owner has access to upload the documents.
When data owner uploads the document and click on submit button. On submit, blowfish algorithm is performed to encrypt the documents.
When user wants to View/Download the documents uploaded by the different data owners. The following steps are:
When client click's on the view/download files, it displays all the documents.
When the client click's on view, it displays title, description, encrypted content to verify whether it is relevant to download.
On reading the title and description client be able to download the document which is decrypted automatically.

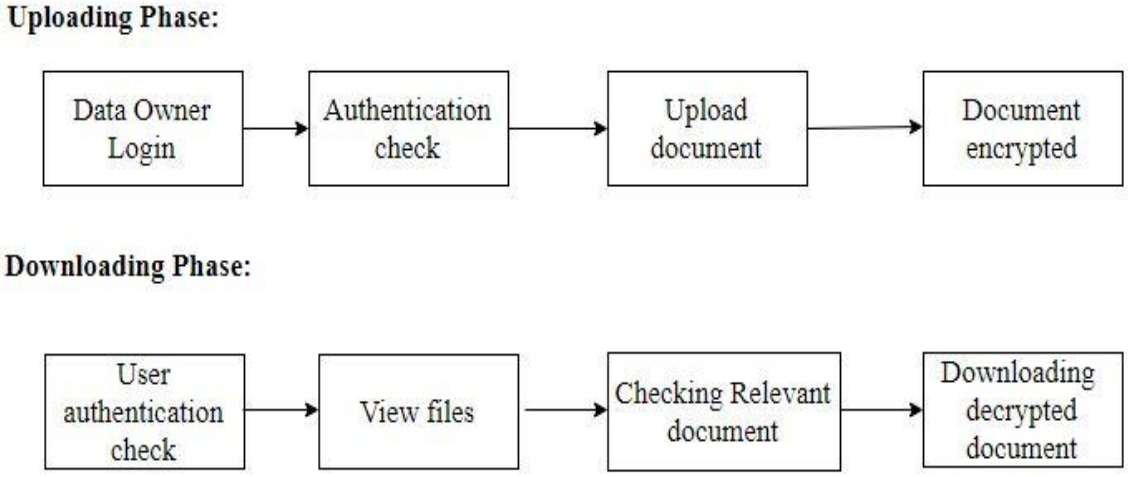


Fig. 5 Working of Blowfish Algorithm

IV. RESULTS

The algorithm is enforced using Java NetBeans and results are implemented in CloudSim. Pdf files are choosing to compute the Time, Decryption time and Encryption time between AES and RSA. Blowfish algorithm is enforced for encrypting and decrypting the documents.

A. Encrypting the document using blowfish algorithm

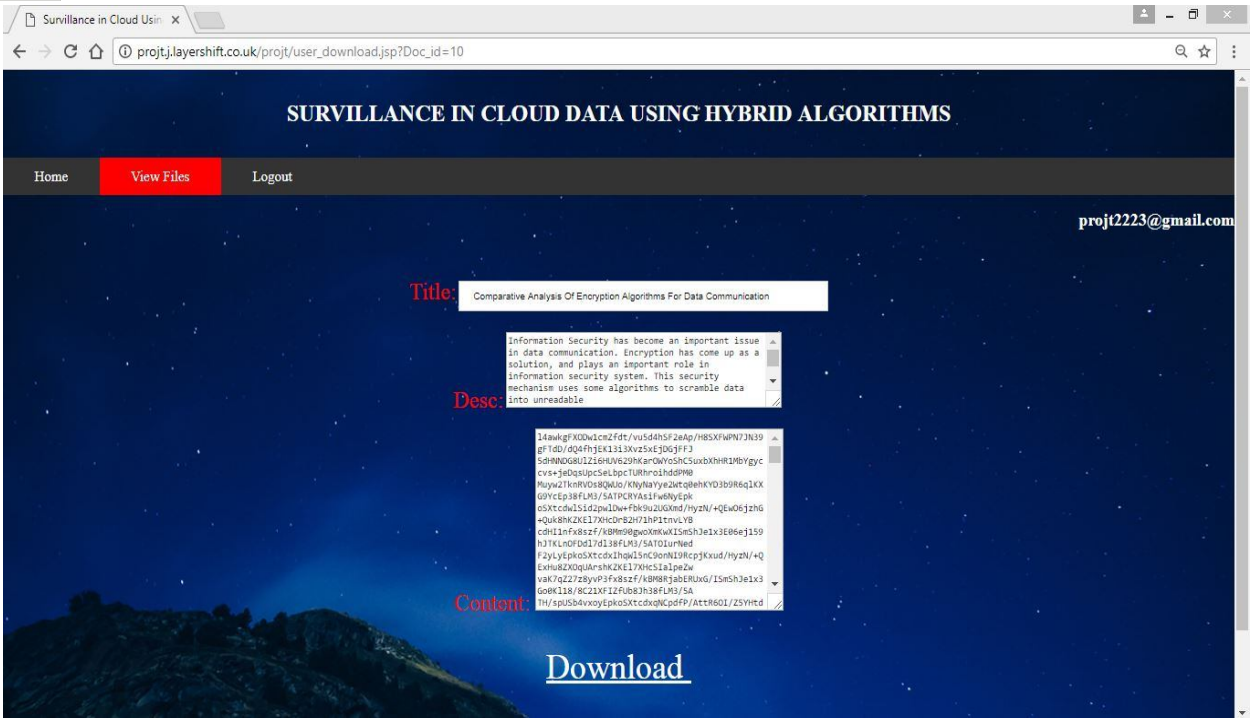


Fig. 6 Encrypting the document using Blowfish Algorithm

B. Calculating the Time of RSA and AES

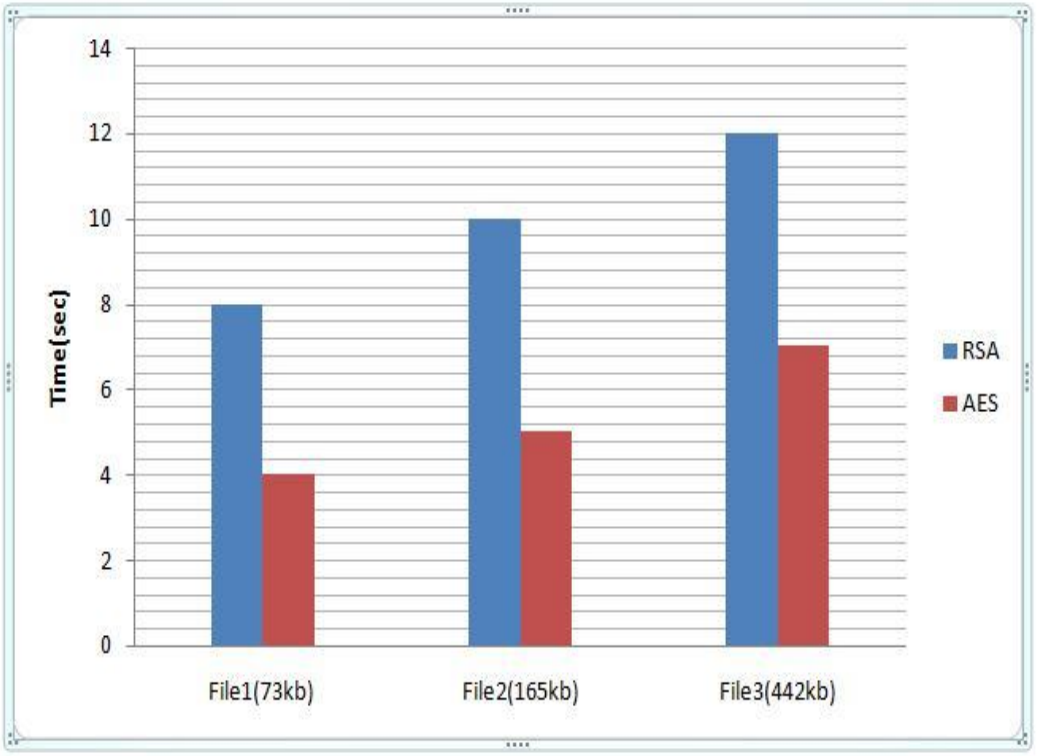


Fig. 7 Compaision of calculating Time between RSA and AES

C. Calculating Encryption time(ms) between AES and RSA

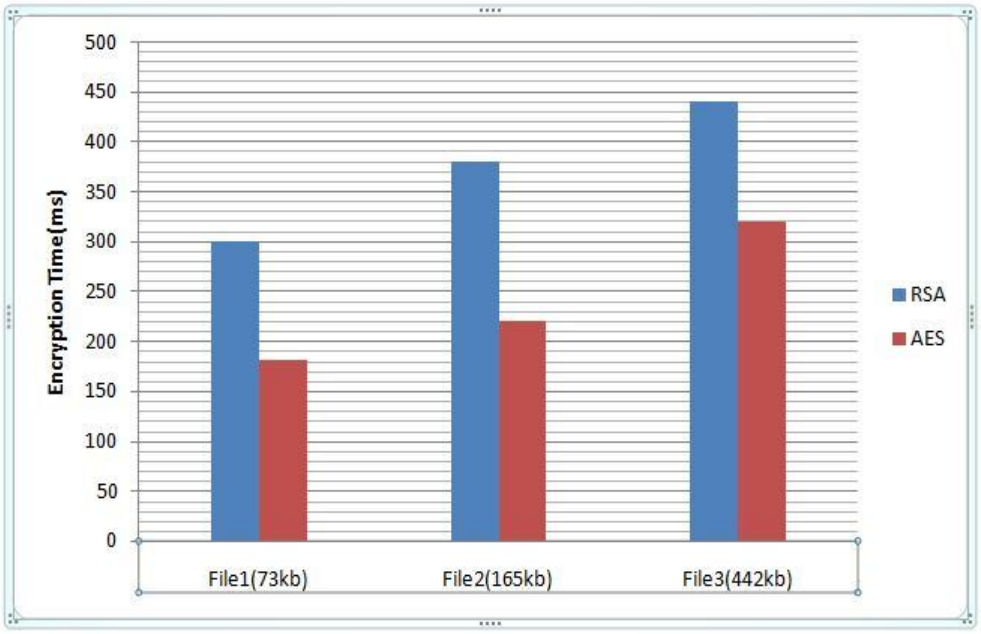


Fig. 8 Comparison of calculating encryption time between AES and RSA

D. Calculating Decryption time(ms) between AES and RSA

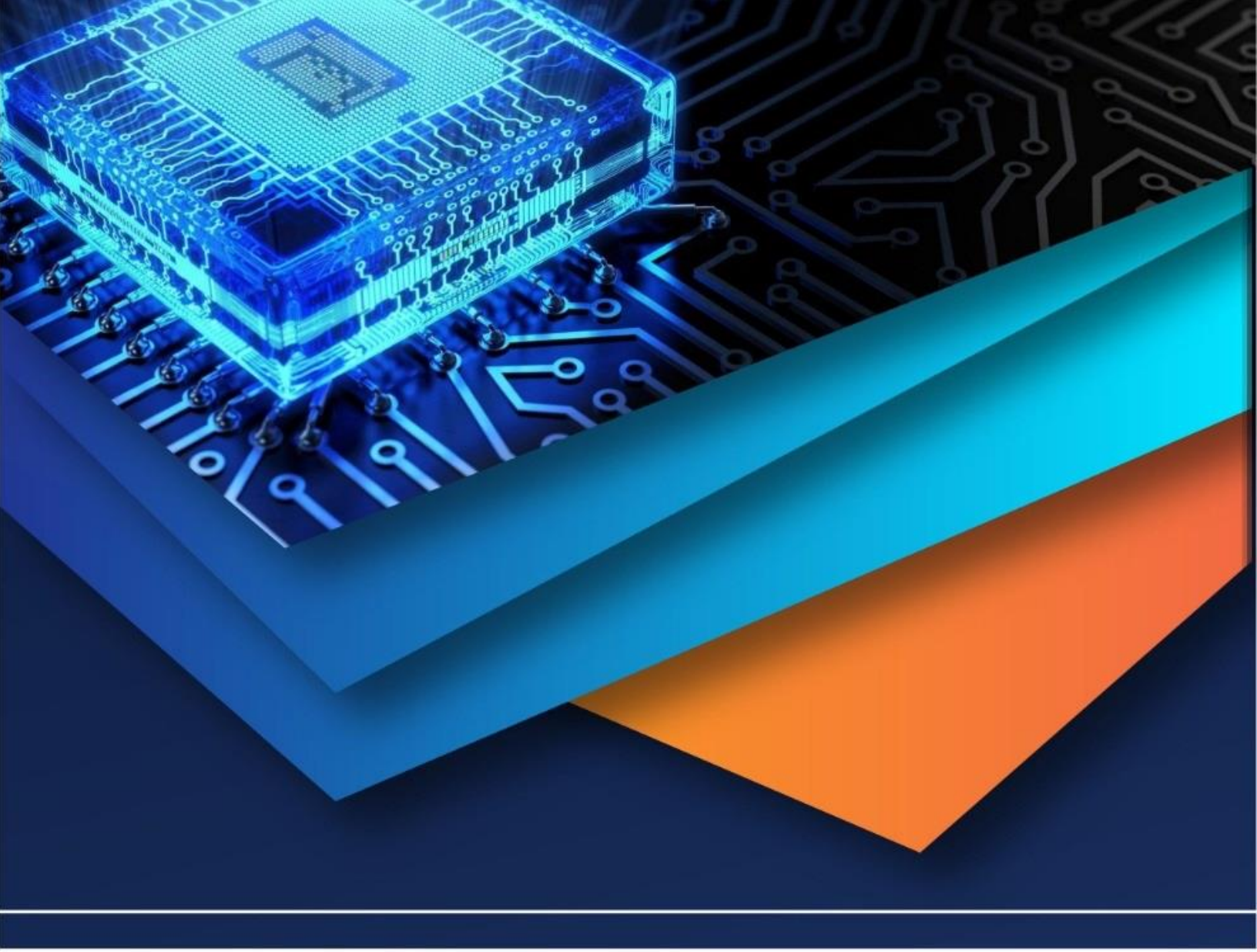
Fig. 9 Comparison of calculating decryption time between AES and RSA

V. CONCLUSION AND FUTURE SCOPE

Security is a most important aspect of cloud computing. To attain security, many cryptographical algorithms are used to decrypt and encrypt the data. The enforced algorithm is a hybrid of 2 algorithms RSA along with Blowfish and AES along with Blowfish. From above results, using large size pdf files based on the parameters of encryption, computation time and decryption time that it can be concluded that AES algorithm is more secure than RSA. Blowfish algorithm is employed for encrypting and decrypting the document because there can be safety breaches or any interloper attack whereas fetching or storing the data.This job can also be extended for audio files , video files and images for encryption and decryption.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cloud_computing.
[2] Kalpana, Parsi, and Sudha Singaraju."Data security in cloud computing using RSA algorithm."(2012).
[3] Saini, Garima, and Naveen Sharma."Triple Security of Data in Cloud Computing.", International Journal of Computer Science & Information Technologies.(2014).
[4] Subhash, Shirole Bajirao. "Data Confidentiality in Cloud Computing with Blowfish Algorithm.", International Journal of Emerging Trends in Science and Technology.(2014)
[5] Sanjoli Singla, Jasmeet Singh. "Cloud data security using authentication and encryption technique". Global Journal of Computer Science and Technology.(2013).
[6] Kumar, K. Vijay, Dr N. Chandra Sekhar Reddy, and B. Srinivas Reddy. "Preserving Data Privacy, Security Models and Cryptographic Algorithms in Cloud Computing."International Journal of Computer Engineering and Applications.(2015).
[7] Jasleen Kaur, Sushil Garg, "Security in Cloud Computing using Hybrid of Algorithms", International Journal of Engineering Research and General Science.(2016).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY