A Secure File Transfer over Virtual Machine Instances using Hybrid Encryption Technique

Dhanush U[1], Prasannasai S Hulikatti[2], Raghavendra H Malager[3], Sandur Shreesha[4], Prakash Biswagar[5]

[1,2,3,4]Student, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA

[5]Professor, Dept of Electronics and Communication, R.V. College of Engineering, Bangalore, INDIA

[1]dhanushu.ec17@rvce.edu.in, [2]prasannasaish.ec17@rvce.edu.in, [3]raghavendrahm.ec17@rvce.edu.in, [4]sandurshreesha.ec17@rvce.edu.in, [5]prakashbiswagar@rvce.edu.in

Abstract: *Cloud Computing is used to share data, services and resources via a network but this system is vulnerable to cyber-attacks by an unauthorized person denying the user privacy and confidentiality. The exponential growth in Information technology especially in the field of Cloud Computing has seen a rise in security attacks such as Interruption, Interception, Modification, Fabrication making it absolutely necessary to enhance the cloud security as well as network security. To tackle the menace of security threats is to make use of the various encryption techniques and to ensure secure transmission of the data to ensure the user of his rights of Privacy, Confidentiality, Integrity, Authentication and access controls of data. This can be achieved by Cryptographic techniques. In the former implementation a new virtual instance is created and embedded with all the requested resources and allocated to the user where as in the later implementation the size of the allotted VM is being altered to account for the extra requested resource or to free the unused resource to increase efficiency.*

To achieve Secure file transfer between instances Hypervisor tool Virtual Box developed by Oracle Corporation is used. To interface with Hypervisor via Host CLI commands provided by the Virtual Box is used. Thus, developing a model that mimics the cloud environment in small scale using the laptop/desktop which enacts as a cloud with limited resource pool.

Keywords: **AES, Blowfish, Cloud computing, Hybrid Cryptography, VM instance**

1. INTRODUCTION

Cloud computing is used to store data which facilitates the user on-demand access of the data stored. Under the current circumstances of the Pandemic and most organizations shifting to work from home, there has been a huge leap in the demand for such cloud computing services. This has resulted in steep rise in data being stored in the cloud, making it absolutely necessary to ensure data security in addition to this cloud computing lie also provides Reliability, Scalability, and Elasticity of resources which makes cloud computing be accessible to anyone on internet to store their data in the cloud. The project makes use of Cloud Computing Virtualization for providing the physical resources, such as processors, disk storage, and broadband network. Virtualization is nothing but a creation of a virtual version of an OS, a server, a storage device, or network resources. Or simply an abstraction of physical resources for users. In the Cloud, these physical resources are regarded as a pool of resources, these resources thus can be allocated on demand. A Virtual Machine is a Virtual Software Computer that, is like a physical computer runs an OS and application. Our design uses IaaS approach. Providers provide Virtual Machine to end user which is used as VM instance to host/run his applications. Many organizations moving towards private cloud for an effective resource utilization, cost reduction, and straightforward maintenances. On an Internet based Cloud platform, owing to the surge in the number of users and the Cyber-attacks, the cloud service provider is compelled to ensure data security of the data to the Users.

To mitigate this problem the technique of Cryptographic Methods is most suited which converts the Message/data into a non-readable form hence, protecting the data from unauthorized parties. This Solution can be exercised with the help of either Symmetric or Asymmetric key Cryptographic Techniques. Symmetric key Algorithms use only one key for the processes of Encryption as well as decryption, whereas Asymmetric key Algorithms depend upon 2 keys i.e., a public key and a private key for the processes of Encryption and decryption. This paper talks about a cost-efficient method to simulate a Cloud Environment using Virtual Machine instances and Various methods to ensure access of data only to authorized users. Data is secured by using a Hybrid Encryption method where the message is split into two parts. The First part is encrypted using AES and the other part using Blowfish Algorithm. It concentrates on 2 block ciphers which tend to provide more security when compared to Stream ciphers.

The addition of key exchange algorithms like Diffie Hellman make the transmission of the key from the sender to the receiver more secure and reliable. Making sure that the data is only accessed by authorized users is also important, which can be mitigated by techniques such as Digital signature. This would ensure that the user exercise full control on the data being transferred over network.

2. LITERATURE REVIEW

To get the idea for different frameworks that provide solutions [1] gives a new original method for cloud storage and for protecting the organizations' data. This proposed system provides an increased level of authentication with the help of AES and time-stamping algorithms. The experimental results illustrate the efficiency of the proposed method when auditing the integrity of the shared data. While [2] presents a framework with key features including enhanced security and owner’s data privacy proposed algorithm involves less power consumption, better load balancing, and enhanced trust and resource management on the network. The results show that the framework proposed minimizes energy consumption by 14.43%, network usage by 11.53%, and delay by 15.67%.

In addition to solutions knowing, how it conventionally works is important. [3] explains in detail how data is securely transferred on cloud. It discusses the various techniques that help achieve good amount of security which include Forward security, Backward security etc. The energy consumed is reduced using Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Data centres.

After the system changes, cryptographic techniques are taken into consideration. [4] focuses on securely storing information into the cloud, by splitting data into several chunks and storing parts of it on cloud in a way that preserves data confidentiality, integrity and ensures availability. It stores the client sensitive information data across single cloud, using AES, DES and RC2 algorithm. Thus, ensuring the security and privacy of the client.

While [5] introduces a new security mechanism using symmetric key cryptography algorithm and steganography. This proposed system uses AES, blowfish, RC6 and BRA algorithms to provide block wise data security. [6] presents a Hybrid encryption algorithm to safeguard data security in Cloud. The algorithm is a hybrid of AES and RSA. Security is the most important factor in cloud computing, and hence is dealt with great precautions. This paper mainly focuses on the following three tasks:
1. Secure upload of data on cloud such that even the administrator is unaware of the contents of data.
2. Secure download of data in a way that maintains the integrity of data.
3. Proper usage and sharing of the public, private and secret keys involved in encryption and decryption.
As pure crypt techniques come with their own merits and demerits [7]. shows how various existing solutions that use pure cryptographic techniques to mitigate security and access control problems suffer from heavy computational overhead on both the data owner and cloud service provider for key distribution and management.
[8] introduces a new advanced security architecture for user identification which includes two factor authentications, AES based file encryption and decryption of data uploaded on cloud, admin verification, locking of users, fetching IP details of users and distributed database storage. Distributed database storage means that data is stored in tiers which means user login details is stored in one database &encryption/decryption details such as files uploaded and key is stored on different database.

The next step to making a hybrid algorithm is to choose the best for this we look into [9]. focuses on the view of DES, AES and RSA as the major cryptographic techniques, and how these crypt techniques secure the data by the use of encryption and decryption. This paper takes a literature survey and also compares the relationship between DES, AES and RSA crypt algorithms, as they are one of the significant modules to secure and/or the messages using crypt file keys. In addition to the previous we also refer to [10] which talks about AES. Advanced Encryption Standard is one on the most regular and mostly symmetric block cipher algorithm. This algorithm has a specific method to encrypt and decrypt subtle data and is put in all hardware and software. It is very difficult to crack for hackers and provides high security. Till date there is no proof of this algorithm being cracked. AES has the capacity to deal with 3 dissimilar key sizes such as AES 128, 192 and 256 bits. Each of its code has 128 bits.

3. COMPARATIVE ANALYSIS FOR BEST ALGORITHMS

The paper emphasizes on a Hybrid cryptographic method. A Comparative Analysis was run to ensure that we had 2 algorithms which were efficient and provided a high level of security. The Methods chosen for the analysis are Advanced Encryption Standard (AES), Data encryption standard (DES), RSA, Triple DES and Blowfish Algorithm. The Results are as in the bar graph in Figure 1.

From the results it is crystal clear that the 2 algorithms which best match our needs are AES and Blowfish. Both the methods are efficient and provide a good level of security.

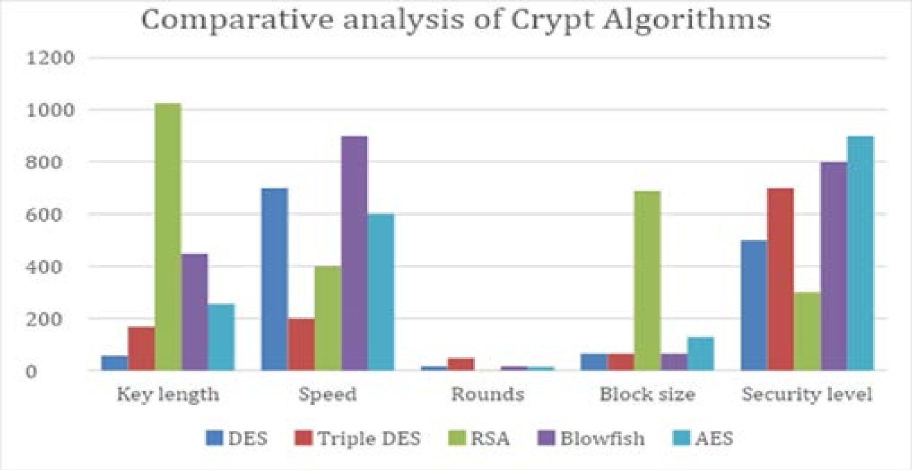


Figure 1. Bar Chart for Comparative Analysis

ADVANCED ENCRYPTION SYSTEM(AES)

AES is a block cipher in which the size of the plaintext and cipher text is the same. The size of the key used depends upon the number of rounds run here, we processed a 128-bit key hence we have 10 rounds in encryption. The message is

converted into hexadecimal values and then the plaintext is converted to matrix form. Then we have the 10 encryption rounds it is not completely different.

In each round there are 4 steps-

- Sub Bytes: In AES we have a 16x16 matrix called the S-box which contains permutations of all possible 256, 8-bit values. The Row and Column serves as indexes into S-box to select a unique output value. S-box has been created by taking Affine transformation with the help of a 8th order irreducible polynomial. Inverse S-box is calculated by taking Inverse Affine transformation of output value followed by Multiplicative Inverse.
- Row Shifting: In Row 1, there is no shifting. In Row 2, there is 1-byte left shift. In Row 3, there is 2-byte left shift. In Row 4, there is 3-byte left shift.
- Mix Column: The state array is multiplied with a pre-defined matrix to get a new stare array.
- Add Round Key: Similarly, we have 10 such rounds. Inverse of this process gives us the decrypted data back.

BLOWFISH

Blowfish is a symmetric encryption algorithm, also a block cipher. The block length for Blowfish is 64 bits and variable key length of 32 bits to 448 bits. It has a total of 16 rounds with 18 sub keys of 32 bits which are generated by performing XOR operation on permutation box and key.
For encryption 64-bit block is divided in to 2 parts, in each round left part is XORed with sub keys and passed through a function where it is divided into 4 parts and expanded using 4 Substitutional box and operation is done to get 32 bits and it's swapped with right part. After 16 rounds Left and right parts are XORed with remaining 2 subkeys and combined and the reverse process is followed for decryption.

A Hybrid cryptographic method was then developed using Python. In the Hybrid Encryption method, the message is split into two parts. The first part is encrypted using AES and the other part using Blowfish Algorithm. Also, Diffie Hellman Key exchange Algorithm was implemented. Diffie Hellman is not an encryption algorithm, rather it uses asymmetric encryption to exchange a secret key between the two users OSs where the file transfer is taking place.

4. IMPLEMENTATION

The paper analyses the entire cloud behaviour being deployed via Virtual Machines strategy wherein the cloud server is represented by a local PC (Host OS) and an open-source Hypervisor (Virtual Box) to deploy instances that act as individual users (Guest OS). Database of Customer activity is maintained to keep track of the VM allocation details and recent activity of the user.

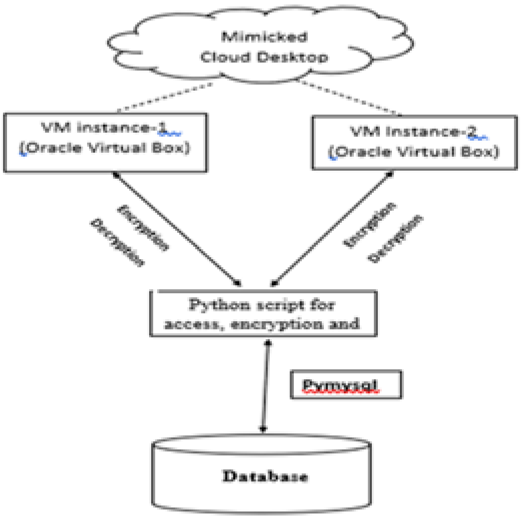


Figure 2. Block Diagram Representation of Implementation

The design customs a Shared folder mechanism provided by Virtual Box to transfer files between server and client in addition to this a Vertical Scaling strategy is utilized to optimize the requirements for instances of VM for effective deployment of design. All the modules are scripted with Python for effective file handling. To handle database creation the XAMPP software's Apache server that runs on localhost IP address (127.0.0.1).
The user interface is provided with command line prompt of the desktop/laptop to interact with python script and perform the operation as per requirement. The CLI commands provided by the Oracle Virtual Box software are used to perform the scaling by embedding those commands into the python script. To embed these CLI commands into the python script 'OS' and 'subprocess' modules are imported to the python script. The

module is subdivided into several functions that perform different tasks requested by the user and thereby making any debugging or any future changes easier and those options are as listed below: -

- Allocation
- Deallocation
- Scaling
- File Transfer

The implementation Code uses "Universally Unique Identifier (UUID)" a 128-bit label used for information in computer systems to access each of Virtual Machine and any operation to be performed is done via UUID and these could be gained via CLI command provided by VirtualBox.

vboxmanage showvminfo "Name of machine"

A. Allocation

The method used to run a VM instance if not powered, else assuming the user requested to restart, the instance is powered off and replayed. If none of the default values are set, the GUI variant will be started.

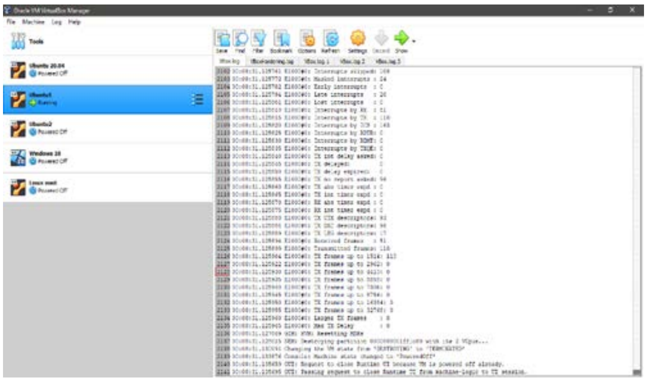


Figure 3. Running Status of VM Instance

vboxmanage modifyvm 'VM_name/UUID', the command starts a VM that is currently in the Saved states or Powered Off.

B. Deallocation

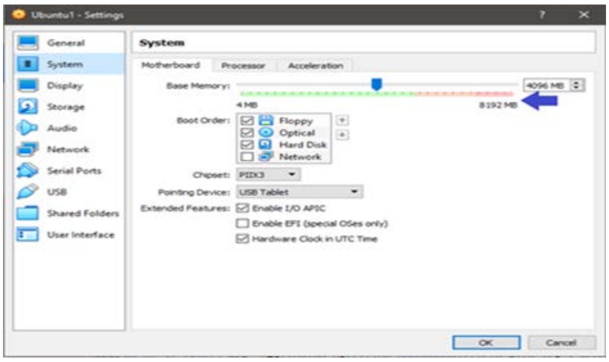
The function used to power off VM if in running state After this, the VM's state will be Powered Off. From that state, it can be started again. and provides an error message if the instance not in a running state.

vboxmanage controlvm 'VM_name/UUID' poweroff, the command has the same effect on a virtual machine as pulling the power cable from PC. Data may be lost if state of the VM is not saved beforehand, this is equivalent to selecting the close-in machine menu of the GUI and then selecting Power Off the Machine.

C. Scaling

In our design, scaling provides optimization to design implemented by modifying the parameters of instance depending on usage of Guest OS and requirements of the file to be transferred over Host OS. The scaling range provided is limited by the desktop/laptop specifications on which the scaling model is being implemented.

- The RAM can be scaled for all the VMs as per usage but while implementing the sum of all the RAM space for all the running VMs at any point of time should be less than critical usage of Host OS in order to ensure smooth and flawless implementation.



Base Memory: 4096 MB

Boot Order: ☑ Floppy ☑ Optical ☑ Hard Disk □ Network

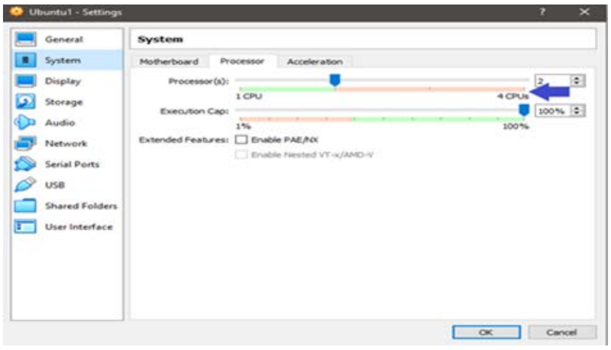
Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features: ☑ Enable I/O APIC □ Enable EFI (special OSes only) ☑ Hardware Clock in UTC Time

Figure 4. RAM Resizing based on Requirement

- The number of CPUs can be allotted for all the VMs depending on the requirement. Here too it should take care that the sum of all allotted numbers of CPUs of all the running VMs is less than critical usage of Host OS.



Processor(s): 2

Execution Cap: 100%

Extended Features: □ Enable PAE/NX □ Enable Nested VT-x/AMD-V

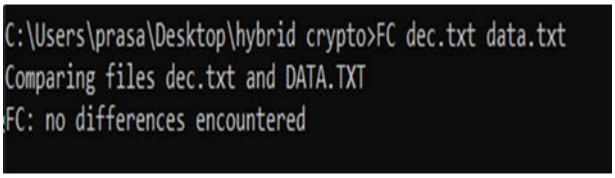
Figure 5. Number of CPU Allocated

The scaling action is triggered by the user from the command-line interface (CLI) which is interfaced with python via the "subprocess" module. The properties altered by this command correspond to the VM settings displayed in each VM's Settings dialog.

- *vboxmanage modifyvm 'VM_name/UUID' --memory 'size_in_MB'*, the command is to set the amount of RAM, in MB, that a VM should allocate for itself from the host.
- *vboxmanage modifyvm 'VM_name/UUID' –cpus 'number'*, command is to set the number of virtual CPUs for the virtual machine, Sets the maximum number of virtual CPUs that can be plugged into the virtual machines if CPU hot-plugging is enabled. This command changes the properties of a registered virtual machine that is not running else the running VM instance is turned powered off and the scale function is called.

D. File Transfer

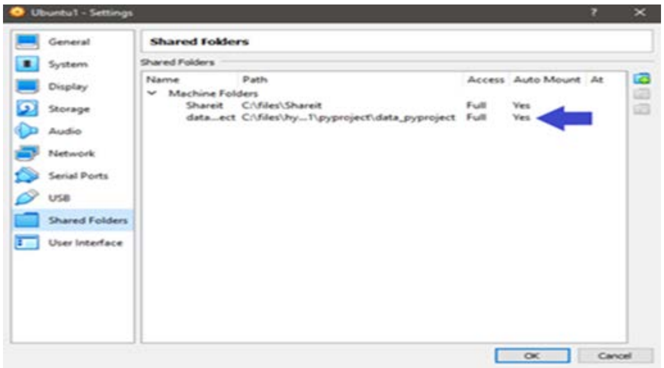
Shared folders enable the user to share data between the Host OS and guests. which can be accessed if Oracle VM VirtualBox Guest Additions software is installed on the guest OS. The shared folder is associated with a share name and the full pathname of the folder or directory on the host system. Our design uses this mechanism to share folders between different instances of VM, where the data to be transferred to destination is dropped into a particular directory that is shared with Host OS.



```
C:\Users\prasa\Desktop\hybrid crypto>FC dec.txt data.txt
Comparing files dec.txt and DATA.TXT
FC: no differences encountered
```

Figure 6. Comparing the Data between Sent and Received Files

Data received is split into two where the first half is encrypted using AES and other half using Blowfish. Key is shared between two instances and decryptor function in relation with receiving Guest OS uses the received key to decrypt encrypted data. The decrypted data is then sent to a directory that is shared with the destined guest OS thereby maintaining security on data being transferred between two guest OS. Here Host OS acts as cloud and each Guest OS as Individual User provided that both encryption and decrypted in Host OS and the process is completely hidden from Guest OSs mimicking actual working of Cloud environment.



Shared Folders

Shared Folders

Name	Path	Access	Auto Mount	At
Machine Folders				
Shareit	C:\files\Shareit	Full	Yes	
data...ect	C:\files\hy...1\pyproject\data_pyproject	Full	Yes	

Figure 7. Shared Folder between Host OS and VM Instance

- *vboxmanage sharedfolder add 'VM_name/UUID' --name 'Name of folder' –hostpath 'Hostpath directing to folder' —-'attributes' –automount*, shared folder add command creates a shared folder which is specified on the host computer. When configured, the contents of the folder on host system can be shared with the guest OS.
- *vboxmanage sharedfolder remove 'VM_name/UUID' --name 'Name of folder'*, shared folder remove command removes a shared folder created

5. CONCLUSIONS AND FUTURE SCOPE

With the global network leaders are shifting their entire infrastructure to the cloud. It becomes necessary manage the cloud environment efficiently and manage the dataflow between network to get more throughput. Pure cryptographic algorithms provide their own set of merits and demerits but mainly focusing on security. But coming to cloud environment there has to be trade off to be made as encryption and decryption constitutes a certain amount of computational overhead as well. The report focuses on representing a Bare metal Hypervisor in terms of Type II hypervisor in an efficient way possible via integration of Shared Folder provided by VirtualBox and Hybrid algorithm to secure transfer of files between Guest OS to mimic cloud environment

Cloud network currently being deployed is actually an infinite resource pool but in our mimicked model where resources are limited by physical system i.e., Host OS. The results obtained showcase a small mimicked model can handle all edge cases which can occur in the real-world scenario. Hence, the project can be extended to the large-scale requirements and overheads in an actual cloud environment with some adaptable modifications. Container-based implementation can also be used for proposed design with some major changes. A container is software that packages code and its resources in a single package so that applications can be easily deployed with less storage consumption as containers can run multiple loads on a single OS instance where as in VMs the hardware is being virtualized to run multiple OS instances.

ACKNOWLEDGEMENT

We would like to express our gratitude to our guide Dr. Prakash Biswagar for guiding us in each step of project.

REFERENCES

[1] R. Sheeja et al, “Secure File Sharing System in Cloud Using AES and Time Stamping Algorithms”, IOP Conference Series: Materials Science and Engineering.,2020

[2] Fijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, and Allah Ditta,” Secure Framework Enhancing AES Algorithm in Cloud Computing “ -Security and Communication Networks Volume 2020

[3] Muthi Reddy P. A, Manjula S. H. b, Venugopal K. R “Secure Data Sharing in Cloud Computing: A Comprehensive Review”– International Journal of Computer, Volume 25, No 1, pp 80-115,2017

[4] Joseph Selvanayagam, Akash Singh, Joans Michael, Jaya Jeswani “Secure File Storage On Cloud Using Cryptography”, International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 03. 2018

[5] Punam V. Maitri, Aruna Verma,” Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm “, IEEE WiSPNET 2016 conference

[6] V.S. Mahalle , A. K. Shahade, “Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm”, IEEE, INPAC,pp 146-149,2014

[7] K. S. Wagh, Rasika Jathar, Sonal Bangar, Anu Bhakthadas, “Securing Data Transfer in Cloud Environment”, Int. Journal of Engineering Research and Applications,2014

[8] Sanjay Kumar et al ,” A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing”, International Conference on Mechanical and Energy Technologies (ICMET),2019

[9] M.Kannan , Dr.C. Priya, S.VaishnaviSree, “A Comparative Analysis Of Des, Aes And Rsa Crypt Algorithms For Network Security In Cloud Computing", Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6, Issue 3,2019

[10] Prof. S. Delfin, Rachana Sai. B, Meghana J.V, Kundana Lakshmi. Y, Sushmita Sharma,” Cloud Data Security Using Aes Algorithm “International Research Journal of Engineering.