

MINOR PROJECT

DATA SECURITY IN THE CLOUD COMPUTING ENVIRONMENT USING CRYPTOGRAPHY

MENTOR: Dr. Suyel Namasudra

MEMBERS:

Devansh Jain (1806174)

Mrinal (1806149)

Gaurav (1806146)



INTRODUCTION



1. Cloud computing is delivery of computer services such as servers , storage, database , networking , analytics and more over the Internet.
2. It provide an alternative to the on-premises data centre , which saves a huge cost and work.
3. Public cloud , Hybrid cloud and Private cloud are three types of cloud computing .
4. Our project consists of designing a new approach that combines Cloud Computing and cryptography.



ADVANTAGES

1. It reduces huge capital cost buying hardware and software .
2. Resources can be accessed very quickly .
3. Productivity is high as we have to put less operational effort.
4. Backup and recovery of data are less expensive and very fast.
5. We can increase or decrease requirement of resources.

DISADVANTAGES



1. You can't do anything with cloud as long as your internet access is out.
2. From an angle security is also an issue with cloud computing.
3. There is a possibility that your cloud service provider run out of money and closes their doors forever.



APPLICATION

1. Art applications like Moo, Adobe creative cloud , Vistaprint.
2. Business applications like Salesforce , PayPal etc.
3. Data storage and backup applications.
4. Educational Applications .
5. Entertainment applications like online games.
6. Management applications .

MOTIVATION



- Cloud computing helps startups manage shifting computing requirements by providing flexibility in computer service they purchase.
- Cloud has a strong impact on company budgets, it improves use of resources reducing IT spending by 20 and 80%.
- It allows for the possibilities to generate new income streams via the implementation of disruptive business models.
- It allows a greater flexibility in the deployment of services, which permits a “granular” focus in completing or replacing capacities.

TERMINOLOGIES



- **Cloud** : Technology that allows us to access files/services through internet.
- **Firewall** : A defensive technology to keep bad guys out .
- **Encryption** : Process of encoding data with a key to prevent theft.
- **Exploit** : A malicious application or script used to take advantage of user.
- **Breach** : The moment hacker successfully exploits a vulnerability of computer .

AGENTS INVOLVED



- There are various agents involved in the process of data sharing:

1. **Server:**

A cloud server which stores all the information regarding the keys. During the time of data sharing, it helps to validate the user using the key pair generated. If the user is valid, a secure connection is established for the data transfer.

2. **Data owner:**

Data owners or service providers, are those who are the owner of the data. They store either the normal data or the entire database and depend on the server to manage data.

3. **Client:**

Users are the authorized parties who could have access to the data if the server establishes connection between them.

LITERATURE REVIEWS



Algorithms for cloud computing :

D-H:

- It used cryptography keys over a public network, enables two users over a untrusted network.
- It needs two prime numbers , one Prime(P) and another (G) a primitive root of P which is why it has a high computing complexity.

Blowfish algorithm:

- The most common public algorithm . It uses Symmetric cryptography but key is very large .
- In this data is divided into two parts and respective processes are followed on both parts of the message.

Our Project:

- Our project inspired from asymmetric cryptography uses RSA algorithm for key encryption-decryption and AES algorithm for message encryption-decryption .
- Our's is window based application using Java swing as frontend.

SHORT COMINGS OF THE LITERATURE REVIEWS

- Often fails to provide details of the overall strategy.
- Often lack details on how the analysis was conducted.
- Often very time consuming.
- Literature reviews require a good supervision.
- Google search doesn't show relevant information/result.

PROBLEM STATEMENT



- The amount of data produced and stored in computing devices is increasing at an alarming rate.
- Tremendous amounts of critical and sensitive data are transmitted between all these devices.
- Thus, it is very imperative to guarantee the security of all these indispensable data.
- Cryptography is the best way to secure data.
- Therefore build a project for **DATA SECURITY USING CLOUD COMPUTING USING CRYPTOGRAPHY.**



PROPOSED SCHEME

- The objective of the proposed scheme is to develop a highly secured system for data transmission from a sender to a receiver. There are three entities in the proposed system:
 - 1) **Key-Pair Generator:** This entity provides the public and private keys to the sender and receiver during the registration process.
 - 2) **Sender:** This entity stores confidential or normal data.
 - 3) **Receiver:** This entity sends requests to the sender for accessing any required data.

- **SYSTEM SETUP PHASE:**

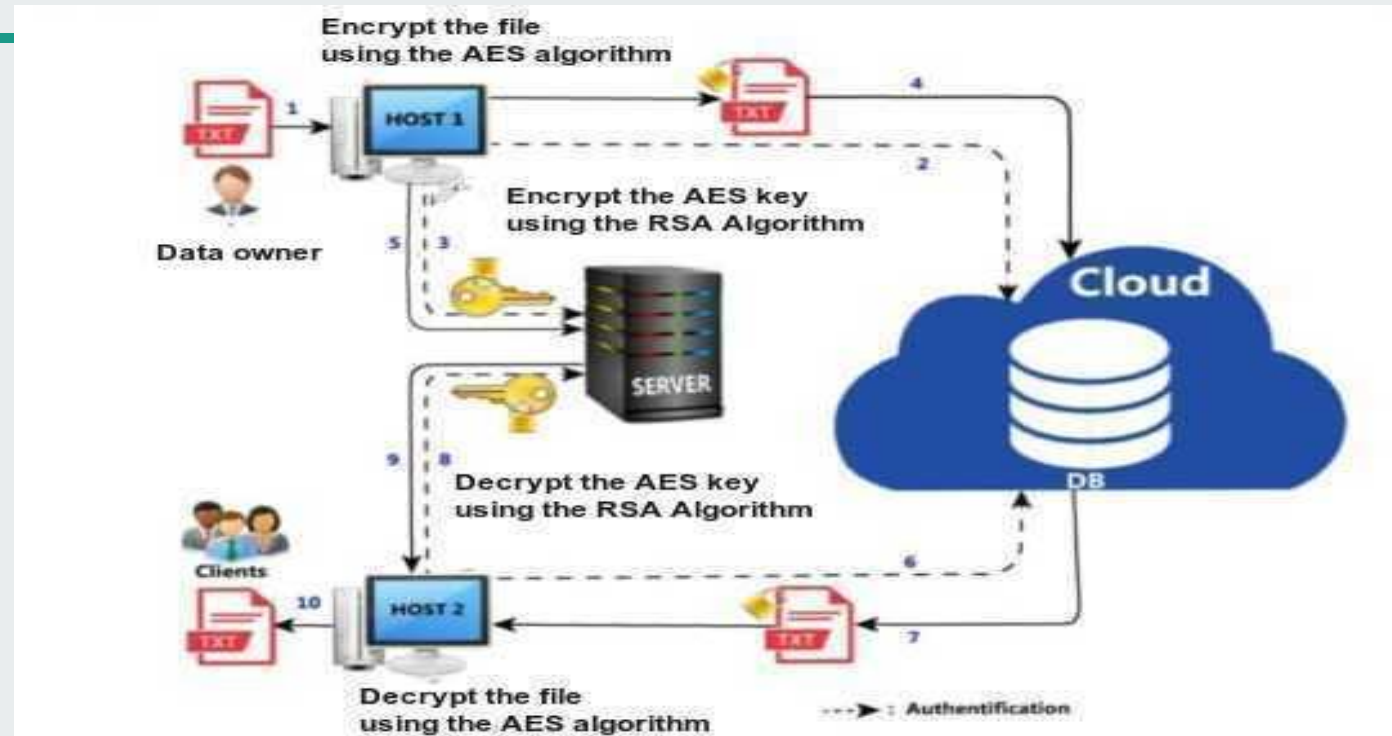



FIGURE 1: Workflow our proposed scheme

- 
- Java Windows Application is being implemented for our project using java programming language.
 - AES Algorithm is used to encrypt and decrypt the text using the key.
 - RSA Algorithm is used to encrypt-decrypt the text of the key when it is shared with the receiver by the sender.
 - Swing is the gui widget toolkit for java which is being used for our project development.

- 
- **Steps to work on RSA Algorithm which is used in key generation:**

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q , and then calculating their product N , as shown –

$$N = p * q$$

Here, let N be the specified large number.

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than $(p-1)$ and $(q-1)$. The primary condition will be that there should be no common factor of $(p-1)$ and $(q-1)$ except 1



Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key

Private Key d is calculated from the numbers p , q and e . The mathematical relationship between the numbers is as follows –

$$ed = 1 \bmod (p-1)(q-1)$$



NOTE:

Encryption Formula: $C = P \cdot e \bmod n$

Decryption Formula: $\text{Plaintext} = C \cdot d \bmod n$

- The details on the working of our application are as follows:

1. AUTHENTICATION

- It consists of two simple input zones.
- One reserved for the user name, the other for the password on which the characters entered are hidden.
- Also there is a button that allows access to the main interface if the password and the login are correct.
- If the password is incorrect then error message will be displayed on a dialog box.

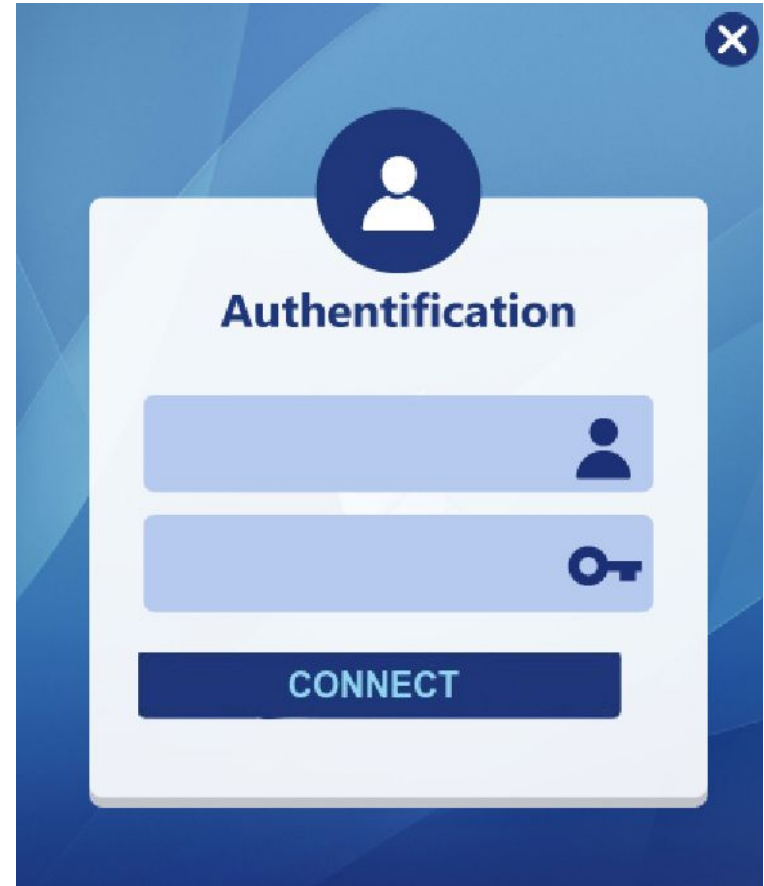


FIGURE 2: Login User Interface



2. HOME WINDOW

- The home window here, is what the window user would interact with as soon he logs in to the application.
- It provides the convenience to the user to navigate to various other features of the application.



FIGURE 3: Home Page

3. CLOUD WINDOW

- In this window the customer can import a file (Word, Text) from his own computer.
- In this case where the customer plays the sender roll, or from the cloud in the case where the client plays the recipient roll.
- In both cases, the customer must import the key or enter it in the key area, to encrypt in the case of an issue.
- After the encryption process, the file should be exported to the cloud.



FIGURE 4: Cloud Window

4. SECURITY WINDOW

- This window is reserved for establishing a connection between the users of the application, in this case the server listens to a connection request.
- After the clients are successfully connected, the transmitter encrypts the key and send it to the server.

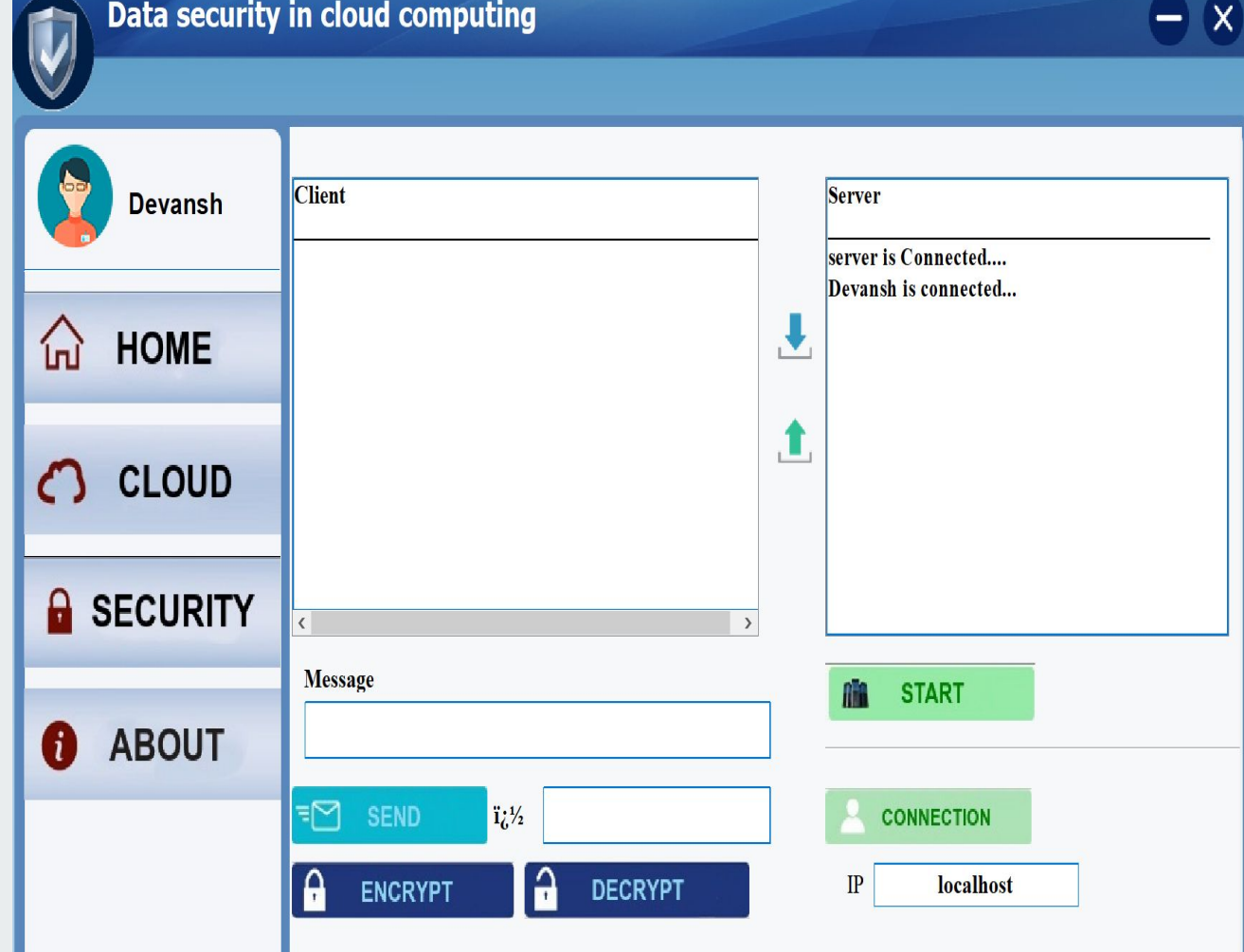


FIGURE 5 : Security Window

EXPERIMENTAL SETUP

(Performance analysis)

The required setup for the development of the project are:

1. **TOOLS:** Apache NetBeans
2. **LANGUAGE:** JAVA
3. **LIBRARY:** Swing.
4. **Hardware:** The project was run on system with following specifications
Processor: Intel i5-8th gen @ 2.3GHz.
RAM: 8GB
HARD DISK: 128 GB SSD

RESULTS AND DISCUSSION



(Performance analysis)

- Successful encryption and decryption of both key and message is achieved verified through decrypting the message and key successfully with respective algorithms.
- Server was starting successfully without any bug at least for what test cases we used.
- Users were connecting successfully and sending encrypted keys to each other over the local cloud.
- User successfully receiving the key and successfully decrypting the encrypted file.
- More complex and efficient user defined algorithm can be developed and used in the project.

CONCLUSION



- Cloud computing here is achieved on local system, using different java libraries and APIs.
- This project is an example for people who still have trust issues on cloud computing for their privacy as this can be extended to a higher level.
- Cloud computing is the future as we don't have to do anything but buy the services, which is a huge advantage.
- Security is still an issue but that will be resolved in coming years.

FUTURE WORK



As we are well aware with the use of DNA computing and it's power to store a large amount of data consuming a very small piece. Using biological molecules to perform calculations rather silicon chips, it could revolutionize the way we store data. So, our future works include:

- Incorporating DNA based data security.
- Implementing a dedicated cloud space rather than local cloud.
- Working and developing a better algorithm for data security, which would be more secure to implement.
- Automating the cloud operations using AWS cloud automation.

REFERENCE

The reference were taken from:

- Towards DNA based data security in the cloud computing environment:
Suyel Namasudra , Debashree Devi , Seifedine Kadry , Revathi Sundarasekar ,
A. Shanthini
- RSA Algorithm:
 - [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
 - https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_understanding_rsa_algorithm.htm
- AES Algorithm:
http://web.mit.edu/6.933/www/Fall2000/aes/AES_final_6933.pdf
- Java and Java Swing:
 - <https://www.javatpoint.com/java-swing>
 - <https://docs.oracle.com/javase/8/javafx/api/javafx/application/Application.html>



THANK YOU!