# A CLIENT SLIDE ENCRYPTION TECHNIQUE IN CLOUD COMPUTING

**BY**

**MD MAHIDUL ISLAM**
**ID: 151-15-5249**

**RIFAT ALI SHAON**

**ID: 151-15-5232**

**AND**

**FAHMIDA YASMIN JEBA**
**ID: 151-15-4859**

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering.

Supervised By

**MD ZAHID HASAN**
Assistant professor
Department of CSE
Daffodil International University

Co-Supervised By

**ABDUS SATTAR**
Senior Lecturer
Department of CSE
Daffodil International University

**DAFFODIL INTERNATIONAL UNIVERSITY**

**DHAKA, BANGLADESH**

**DECEMBER 2018**

# ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **MD ZAHID HASAN**, **Assistant professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*COMPUTER SCIENCE*" to carry out this project. His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to the Almighty Allah and Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

# DECLARATION

We hereby declare that, this project has been done by us under the supervision of **MD ZAHID HASAN, Assistant professor, Department of CSE** and **ABDUS SATTAR, Senior Lecturer**, **Department of CSE,** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

**Supervised by:**

______________________

**MD ZAHID HASAN**
Assistant professor
Department of CSE
Daffodil International University

**Co- Supervised by:**

______________________

**ABDUS SATTAR**
Senior Lecturer
Department of CSE
Daffodil International University

**Submitted by:**

______________________

**MD MAHIDUL ISLAM**
ID: -151-15-5249
Department of CSE
Daffodil International University

______________________

**RIFAT ALI SHAON**
ID: 151-15-5232
Department of CSE
Daffodil International University

______________________

**FAHMIDA YASMIN JEBA**
ID: 151-15-4859
Department of CSE
Daffodil International University

# ABSTRACT

Cloud computing has become the latest technological computing area providing a large number of advantage to the different organization with its different business model at low cost. The main benefit of cloud computing is pay-per-use that means the organization or person do not need to pay any extra cost for the service. So it reduces the extra cost that is a huge benefit of the different organization or the user but this is a matter of security concern that damage the quality of service and a security challenge for cloud computing. The security question is everywhere in the cloud system. It role up data transferring from user to server, server to the user, storing data and retrieving data and meanwhile, it has a great security issue to loss or hacks the data. In this paper, we propose a way to protect the data from hacking or losing when storing or uploading the data in the cloud server using the combination of Advanced Encryption Standard and Secure Hash Algorithm with Initial Vector.

## TABLE OF CONTENTS

# LIST OF TABLE

# LIST OF FIGURES

# CHAPTER 1
# INTRODUCTION

## 1.1 INTRODUCTION

Cloud computing nowadays a big issue in this current development situation all over the world. Cloud computing is a business model that helps all type of organization like small, medium and as well as large organization to use the infrastructure with fast access and support. By the definition of National Institute of Standard and Technology (NIST), cloud computing is a model for empowering omnipresent, advantageous, on-request arrange access to a common pool of configurable registering assets (e.g., networks, servers, capacity, applications, and administrations) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Schematic definition of cloud computing can be simple, such as seen in Figure 1.1

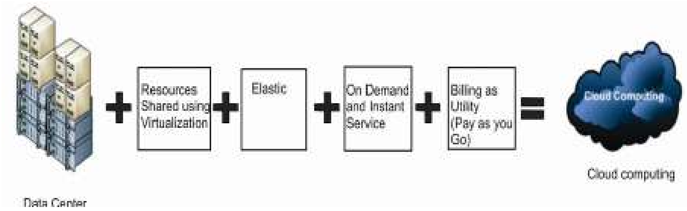

Data Center
+
Resources Shared using Virtualization
+
Elastic
+
On Demand and Instant Service
+
Billing as Utility (Pay as you Go)
=
Cloud Computing
Cloud computing

Fig. 1.1: Schematic definition of cloud computing [1]

About 60% of the business people think that cloud is the best place to stock content and rest of the people, general people, think that cloud is the best place to stock data and retrieve the data virtually [2].

## 1.2 MOTIVATION

Cloud computing is the hotcake today because of its service & functionality. We do not need to carry a lot of cost for using the service, it’s a huge benefit. This service is very flexible, cost-effective and it has a delivery platform to either business or consumer IT services over the internet.  We can access our file or data anywhere in the world. Isn’t it a great thing!

We, in our daily life, use the free version cloud facility like Google Drive and enjoy the benefit of it. Once we tried to know more about the functionality of cloud computing. The journey of study cloud computing, we became impressed. But when knew that there is security concern issue we felt anxiety. Then we decided to find the solution. After studying the issue we realize that if we secure our file before uploading in the cloud it may reduce the problem. And then our journey to study and research about cloud data security.

## 1.3 CLOUD COMPUTING

We already discussed cloud computing means in our previous season. Now there is a question that why cloud computing? Data storage has become a big priority for every computer or mobile users and obviously to main the data a large number of data storage is a need. To maintain the data in a storage the users have to spend a lot of money. But all users even the business owners sometimes cannot effort this amount. Cloud computing minimizes the cost of hardware and software demand of the users. Users now enjoy the benefit of cloud computing like lower IT infrastructure and computer cost, improved performance and platform, instant software update, backup, recovery, performance, scalability and so on. That’s why users are now happy with cloud computing.

### 1.3.1 CLOUD COMPUTING MODELS

There are four types of cloud models: Private cloud, Community cloud and Hybrid cloud. In a private cloud, the computing resources can be owned, organizations or governed. On the other hand, the public cloud the compute resources can be academic, business organization, owned or governed. Next community cloud is for community and organizations. Last hybrid cloud can be used for B2B means business to business.

### 1.3.2 CLOUD COMPUTING SERVICES

Cloud computing services are three types- Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Details are below there of these three services in figure 1.2.

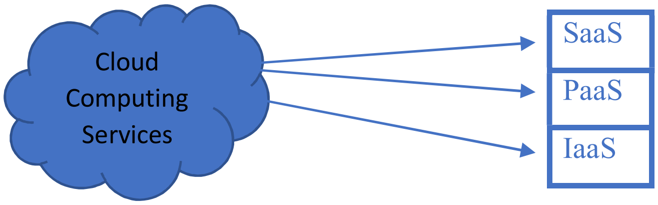


Fig. 1.2: Cloud Computing Services

- **SaaS (Software as a Service)**

SaaS or software as a service is a software distribution model provides an application that is accessible anytime and anywhere in the world. In SaaS applications are hosted by a vendor or service provider and it is available to the customers over the internet. The service is for the end user without requiring installing application on the user's computer. There are so many important tasks can be performed using this application like sales, accounting, invoicing planning and many more.

- **PaaS (Platform as a Service)**

Platform as a service is the middle layer and the PaaS provides a developmental environment to build applications and services to the developer without installing any of these platform and support tools on their local computer. In this service, the support is constantly updated and added new features. Management services, storage, networking, developing, testing, hosting etc. include in this platform.

- **IaaS (Infrastructure as a Service)**

IaaS means Infrastructure as a service provider computing infrastructure like virtual space, balancers, IP addresses, network connections. And this is the lowest layer mainly virtualization technology. The most important news is that Amazon Web Services was the first IaaS provider and remains the leader, followed by Microsoft Azure, IBM Cloud and Google Cloud Platform.

## 1.4 RESEARCH QUESTION

**Question 1:** How to secure data that is stored in the cloud?
**Question 2:** How to secure data when it's stored in the cloud?
**Question 3:** Can we secure the data before and after uploading the data to the cloud?

## 1.5 EXPECTED OUTPUT

We want to secure the data in the cloud. If we take the step to protect the data before uploading it to the cloud then it will be a good solution. We are going to implement a combine encrypted algorithm to protect the data. After uploading, the data can make more secure by taking some authentication step of the user. We are also going to propose a formula or technique to protect the uploading data in the cloud.

## 1.6 REPORT LAYOUT

In chapter-1, we already described of introduction, motivation, cloud computing in details and research question. In chapter-2, we will cover the background of our research in details. Chapter-3 will be about research methodology. Here data security in cloud computing, proposed proposal, implementation requirements and the procedure of data collection will be discussed. Chapter-4 is about the implementation of our work. Lastly, the conclusion and future work will be discussed.

# CHAPTER 2

# CLOUD COMPUTING SECURITY ISSUES AND LITERATURE REVIEW

## 2.1 INTRODUCTION

As a recent phenomenon, in the field of information technology cloud computing is perceived as a virtual cloud with lots of possibilities. The prevalent of distributed computing suppliers are Amazon Simple Storage administrations (S3) and Amazon Elastic Compute Cloud (EC2). Amazon S3 is giving a basic web administrations interface and, whenever, from any area it can store and recover a vast measure of information utilizing the web. Amazon uses to run its very own worldwide system web administrations which can be accessed as it is exceedingly versatile, reliable, fast, economical foundation [3].

Cloud computing providers offer many services to the client and the main feature they provide that is data storage. In this environment, users do not need their own infrastructure even they can use the stored data from anywhere in the world with the help of modern technology. And as there is a pay-per-use policy and users do not need extra costing for using the service it becomes a popular service in the world. But there still some organizations actually not convinced about the service because of proper security control policy.

Stacking basic application and delicate information to the cloud is raised as a noteworthy worry by the associations as the information is moved past their server farm's system which is under their control. Any framework is viewed as secure when all the conceivable dangers or dangers are dispensed with or lessened to the least.

## 2.2 CLOUD SECURITY ISSUES

According to Cloud Security Alliance (CSA), in excess of 70 percent of the world's associations by and by work – at any rate incompletely – on the cloud. With points of interest like lower settled costs, higher flexibility, customized programming revives, extended the joint exertion, and the chance to work from wherever, 70 percent is definitely not a noteworthy astonishment.

In spite of the fact that cloud administrations have introduced another time of transmitting and putting away information, numerous organizations are as yet reluctant or make the move without an unmistakable arrangement for security set up.

Cloud computing is confronting a considerable measure of issues. The issues are recorded as the accompanying: data loss, insecure interfaces, and APIs, malicious insiders, data breaches, data location, and denial of service attack, shared vulnerabilities, hijacking of accounts and abuse of cloud services.

- **Data Loss**

Organizations are re-appropriating their whole data to cloud benefit suppliers. As a result of the ease rate that the cloud offers, the clients should make a point not to uncover their essential data to dangers in view of the numerous approaches to trade off their data. In cloud computing, the dangers are going up on the grounds that there are dangers that is recently confronting the cloud and did not occur to conventional registering, and difficulties taking to keep away from those dangers.

Any data misfortune can speak to genuine harm to the business. Cloud data is liable to indistinguishable dangers from is on-introduce information: unplanned erasure by clients or supplier staff, cataclysmic event, or fear-based oppressor assault. It is the cloud supplier's duty to prepare for the human blunder and to assemble hearty physical server farms.

Notwithstanding, IT should likewise ensure against cloud data misfortune by building up SLAs that incorporate incessant and undeniable reinforcement to remote locales, and encoding records if there should arise an occurrence of unintentional information introduction.

- **Data Breaches**

A cloud circumstance has diverse customers and affiliations, whose data is in a comparable place. Any crack to this cloud the condition would reveal all customers' and affiliations' data to be unclosed. Because of multi-inhabitance, customers using various applications on virtual machines could have a similar database and any corruption event that happens will impact others having a comparative database [1].

One of the examination directed by the Ponemon Institute entitled "Man In Cloud Attack" reports that in excess of 50 percent of the IT and security specialists surveyed believed their affiliation's wellbeing endeavors to guarantee data on cloud organizations are low. In the examination used 9 circumstances, where a data break had occurred, to choose whether that conviction was set up frankly [4].

Resulting to surveying each circumstance, the report contemplated that general data breaking was multiple times more slanted to occur for associations that utilization the cloud than those that don't. The fundamental end is that the cloud goes with an intriguing course of action of characteristics that make it more defenseless.

- **Insecure Interfaces and APIs**

Programming interface keys are utilized by Web and cloud administrations to recognize outsider applications. Web and cloud administrations permit outsider access by uncovering application programming interfaces. In any case, numerous engineers and clients don't sufficiently anchor the keys to the cloud and information. Communication between the cloud service provider and the client through API by which data can be controlled by the clients. Actually, these interfaces should be secure to prevent unknown access. If they are not strong and security mechanism cannot defend them, this could lead to accessing personal information even the user.

- **Malicious Insiders**

A malicious insider is someone (a representative, temporary worker, and so forth) who approaches system and misuses it or takes data, regardless of whether it be for individual gain or vengeance. They will regularly utilize their very own entrance, or if their entrance isn't sufficiently adequate, will attempt and take the accreditations of different representatives. Malicious insiders may attempt and take information, decimate basic data, or discharge private data to people in general.

- **Denial of Service Attack**

Denial of Service (DOS) assaults makes a genuine risk to the cloud. For example, an attacker may use a large volume of the connection request to attack a server. Projects can be intended to send synchronization (SYN) parcels to the objective, which, thus, will answer with another bundle known as SYN/ACK. The server at that point sits tight for a reaction from the beginning framework that never arrives. The false association demand will in the long run time out, however meanwhile, that association isn't accessible to real clients. On the off chance that enough malignant SYN bundles are sent, they can expend the majority of the accessible associations, viably denying any authentic association demands [5].

- **Account/Service Hacking**

Assaults like phishing, misrepresentation and programming abuse are diverse kinds of record/benefit hacking. By and large such movement is completed by taking certifications (accessing one's record unlawfully). Record hacking can make a serious devastation one’s trustworthiness and notoriety.

## 2.3 RELATED WORKS

In the most cryptographic strategies mean to secure information when transmission and capacity. Cloud computing concern the information is put away in Cloud servers or server farms. To give strong security also, security to clients from dynamic, uninvolved assaults the information ought to be scrambled by utilizing symmetric or asymmetric crypto calculations.

Srinivas, Venkata and Moiz give a brilliant understanding of the fundamental ideas of distributed computing. A few key ideas are investigated in this paper by giving models of applications that can be produced utilizing distributed computing and how they can help the creating scene in getting advantage from this rising innovation [5]

B.M Shereek et al in their paper displayed open key cryptographic Calculation that RSA and its security, preferences, assaults on RSA and previous test using Fermats Little Theorem. By testing Fermats Little Theorem in the midst of key age for RSA, the time capriciousness can be decreased since sweeping prime numbers are taken [6].

Sultan Aldossary and William Allen on their “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions” list issues related to data stored in cloud storage and solutions to those issues which differ from other papers which focus on cloud as general [1].

Mr.V.Biksham and Dr. D.Vasumathi discussed encrypted data are proposed using “somewhat” and “fully homomorphic” encryption methods [7]. Eman M. Mohamed, Hatem S. Abdelkader and Sherif El-Etriby had a great discussion about authentication, stronger and faster encryption algorithm, and file integrity on their “Data Security Model for Cloud Computing” [8].

Rachna Arora et al in their paper depicted different calculations like AES, RSA, DES and Blowfish and drew examinations based on time, memory and CPU requirements [9].

Tania Gaura and Divya sharma proposed a model for client-side encryption on their “A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing”. The use AES algorithm with Diffie-Hellman algorithm [10].

Different service provider use different technique for secure data in cloud computing. Most of them do not use client-side encryption.Tresorit, OwnCloud, Viivo different organization use client-side encryption but the encryption keys are on their server, so there is a security concern about the privacy of it [11] [12] [13]

## 2.4 RESEARCH SUMMARY

Related work strategies can give security in cloud computing in the time of information exchange and encryption and unscrambling. In any case, it tends to make more secure and give abnormal state security. In the other part we examine our proposed technique, figure what's more and working procedure. Besides others security issues, the client-side encryption analyzed by the researches and company is given below in the table:

Table 1.1: Summary client-side encryption of different researchers

| Application Name | Encryption Algorithm | License | Features for Storage |
|---|---|---|---|
| Tresorit | AES<br>HMAC-SHA-512 | Unrestricted freeware | 5 GB Free storage |
| OwnCloud | AES | Unrestricted freeware | N/A |
| Viivo | AES | Unrestricted freeware | N/A |

## 2.5 SCOPE OF THE PROBLEM

Our method is well secure to do encryption and decryption. The execution time is also a small amount of time. So, the quality of our model is going to be good. And we can protect users file in cloud computing.

## 2.6 CHALLENGES

We do our research for securing the file before uploading in the cloud. We make a program that encrypts our files. At this moment, giving the professional look of the whole program to user-friendly for common user is a challenge. But our method is strong enough and can secure every file. We will find another solution about security when retrieve the data from the cloud.

# CHAPTER 3
# RESEARCH METHODOLOGY

## 3.1 DATA SECURITY IN CLOUD COMPUTING

In this paper, we mainly demonstrate a secure encryption method to secure data when storing or uploading the data in the cloud server and show an implementation for this technique. In the time of data transmit there is a chance to lose or hack the data. When we upload any data from our device to the cloud, the data then store in the cloud server. After transmit it may also hack the data. If we make the data secure before uploading then it cannot be hack easily. And if the process of protecting data means encryption process is strong enough then obviously it quite impossible to hack the data. The sample process is below figure 3.1:

Fig 3.1: File Encryption before Uploading to the cloud

Then one thing comes out, when we retrieve the data from the cloud server, the data should be the same as before uploading. If we upload the encrypted file then the possibility of hack the data is quite tough but we also propose a way that will be the more secure. If the two way applies to protect the data then there is nothing to worry. It will be the strongest way to protect the data.

## 3.2 PROPOSED METHOD

Our main goal is to protect the data that’s why we make a method that is a combined model using Secure Hash Algorithm and Advanced Encryption Standard Algorithm with an initialization vector (IV). In this method, a random key will generate by SHA and the chosen data file will be encrypted through the AES algorithm. Then the file will be uploaded into cloud. So, there is less possibility to hack the data because the data is previously encrypted with strongest algorithm. Our proposed a combined model using SHA and AES is given below at figure 3.2.

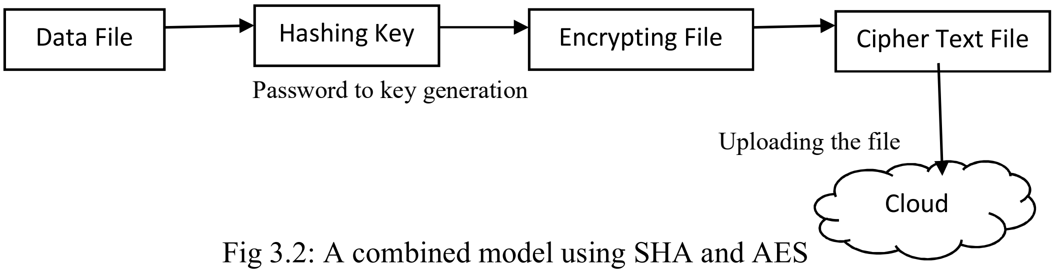


Fig 3.2: A combined model using SHA and AES

## 3.3 WORKING PRINCIPLE

To maximize cloud data security in the time of storing, it's best to consolidate the highlights of these different methodologies. Prior to transferring data to the cloud, first, we encode it utilizing our very own encryption programming. At that point transfer the encoded document to the cloud. Our method firstly generates a secret key against the user's simple password. To encrypt any file we have to first choose the file then have to input a password. If the password is not a big length or strong enough, there is no problem. Because in this method, we use the Secure Hash Algorithm that will create a 32 bytes secrete key against the given password. So, users need not to memories the 32 bytes long key as we use the AES-256 algorithm. After that, the file will be encrypted with the AES algorithm.

## 3.4 IMPLEMENTATION REQUIREMENTS

We implement our proposed method in programming python in PyCharm IDE. PyCharm is an IDE (Integrated Development Environment) used in computer programming, especially for the language "Python". It provides different features like graphical debugger, code analysis, unit test etc. PyCharm is cross-platform, with the versions windows, macOS and Linux.

## 3.5 DATA COLLECTION PROCEDURE

We use a sample data file to testing our method form world data bank. In this site, we select a data file named “popular indicators” from subsection foreign direct investment, net (BoP, current US$). We divided the file to 150kb, 250kb, 400kb and 700 kb to check the execution time also.

# CHAPTER 4

# EXPERIMENTAL RESULT AND DISCUSSION

## 4.1 INTRODUCTION

In the previous chapter, we discuss the model of our proposed method. The model is a combined structured of two different algorithms and IV. In this chapter, the implementation process, output, and the advantage of this method will be discussed.

## 4.2 ABOUT PROPOSED METHOD & IMPLEMENTATION

There are many encryption and decryption algorithm to protect the data in cloud computing. All these cryptographic algorithms are strong enough but we remember that the data can be any type of text, data file, image etc. And there are some also disadvantages of these algorithms. So, remembering this aspect we make our model with the combination of the strongest algorithm AES and SHA. We maintain data integrity in our model. The whole system will be discussed below with the advantages of these algorithms.

- **SECURE HASH ALGORITHM (SHA)**

SHA-256 (Secure Hash Algorithm) is a cryptographic hash function. It takes the text as an input and generates a unique 256-bit (32 bytes) signature for the text. It is not encryption because it cannot be decrypted back. It is called a one-way cryptographic function. For any size of the source text, it will produce a fixed size of hash. SHA-256 is the successor of another cryptographic hash function called SHA-1, and it is the strongest hash function available now. It is a good partner of AES encryption algorithm. In our program, we use it to generate the cryptographic key for our encryption and decryption process.

It generates the key using user password for encrypting any file so the user does not need to remember the long 256-bit key or to store it. It gives more security for the encryption key. It also pretty much impossible to crack so the key is secure.

- **Initialization Vector (IV)**

In cryptography, an initialization vector is blocks of bits that are used to solve cipher text repetition problem. In sometimes during encryption same plaintext encrypted multiple times which produce the same ciphertext. To prevent it initialization vector is used to produce distinct ciphertext. In our program, we use AES-256 in CBC mode which requires a unique binary sequence for each encryption operation and the initialization vector provides it randomly. It also provides security from dictionary attack which is to find a pattern and break cipher. In our program, we use IV of size 16 bytes.

- **ADVANCED ENCRYPTION STANDARD (AES)**

Advanced Encryption Standard (AES) is the most secure symmetric encryption algorithm. It is six times faster than previous generation encryption algorithm triple DES. There are three block ciphers: AES-128, AES-192, and AES-256 from which Advanced Encryption Standard is built. In this algorithm, each of the block ciphers encrypts and decrypts data in chunks of the size of 128 bits by using cryptographic keys. There is three size of cryptographic keys- 128 bits, 192 bits, and 256 bits. The same key is using for both encryption and decryption. Here we used AES-256 for encryption and decryption. For AES-256 there are 14 rounds and each of these round consists of several processing steps including permutation and substitution of the encrypted text, which helps it to turn into its encrypted form. There are five modes of operation in the AES algorithm.

We used CBC (Cipher Block Chaining) mode which is an advanced form of block cipher encryption. In CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point and these add an extra level of complexity to the encrypted data. Performance of AES is very good because it has high speed and low ram requirements. So it performs very well in various types of hardware.

## ENCRYPTION AND DECRYTION PROCESS

In the process of encryption, at first, the user has to select the data file or file by selecting the file name with its extension. Then the user should enter the password, the password can be simple. We recommended password nature can easy to remember. As AES is a symmetric algorithm, it has one key, so with the help of SHA-256 we generate a 32 bytes secrete key and the key is hidden.

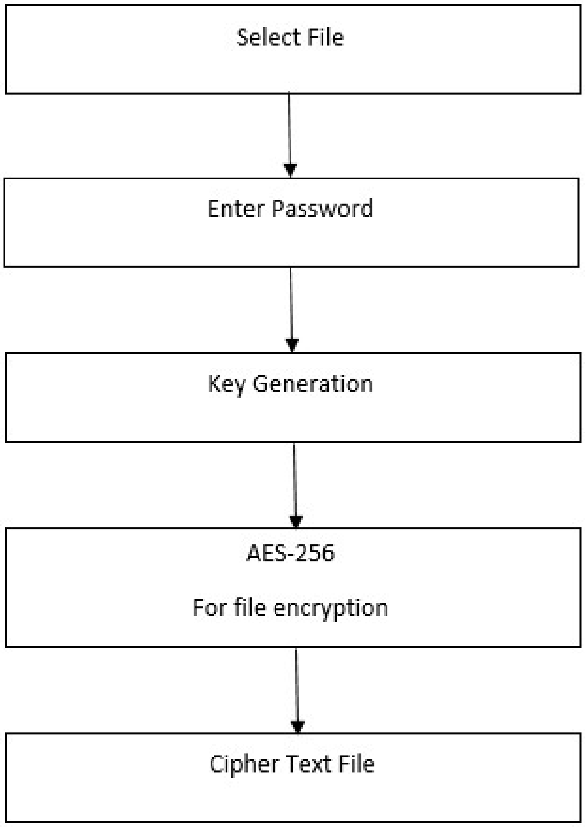


Fig 4.1: Encryption process step by step

No one can find the key even the user. The key will generate against the user's simple password. That's why the user should not remember the actual 32 bytes key to decrypt the file again. The flowchart figure shows the step by step encryption of our proposed method at figure 4.1.

Here we use the initialization vector (IV) that will help to generate a random secure key and the key do not match any other key in this algorithm. If an attacker wants to take decision for the dictionary attack, he/she cannot get success because of IV. After putting the password and pressing enter the file will be decrypted with the functionality of the AES-256 algorithm.

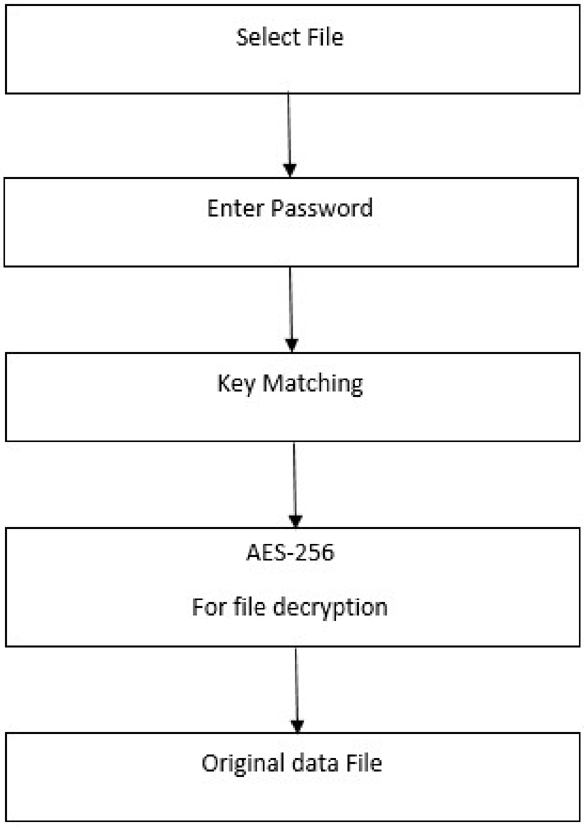
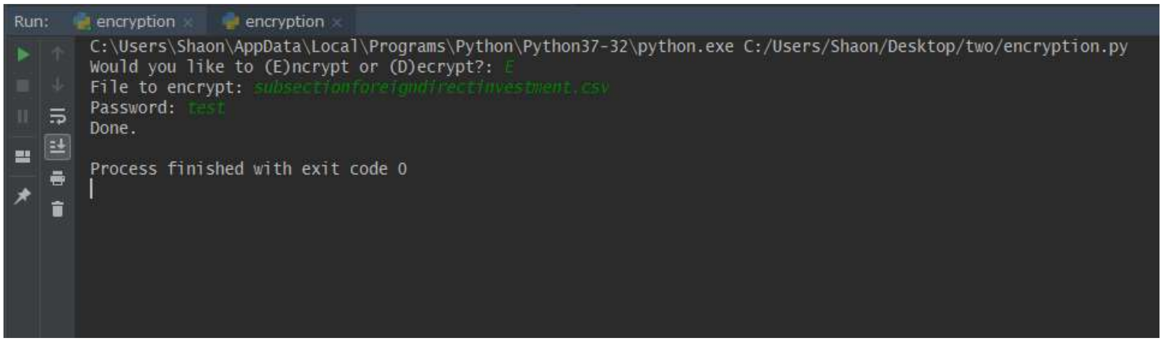


Fig 4.2: Decryption process step by step

The above flowchart figure 4.2 shows the step by step decryption of our proposed method. In this process, the user should enter the file name of the encrypted file. Then have to put the simple password (the password he/she used duration encryption the file), then SHA-256 mass the key and with the process of AES-256 algorithm user can successfully decrypt the file again.

### 4.3 EXPERIMENTAL RESULT

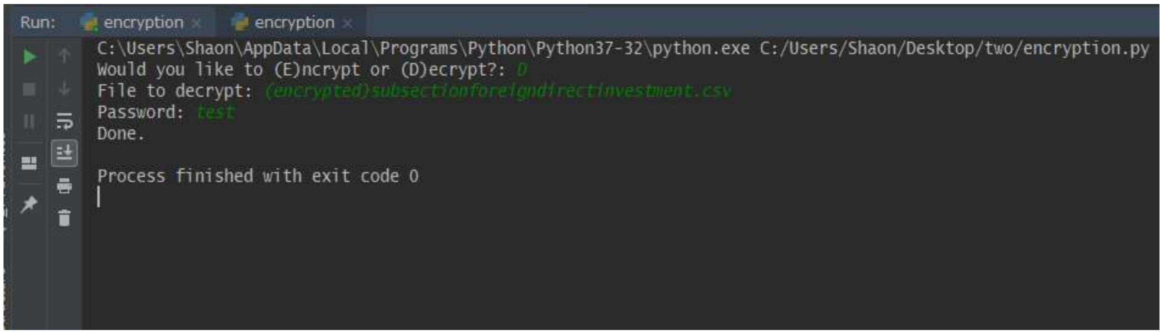
The following figure 4.3 and figure-4.4 show our implemented output, the first one is for encryption and the second one is for decryption.



```
C:\Users\Shaon\AppData\Local\Programs\Python\Python37-32\python.exe C:/Users/Shaon/Desktop/two/encryption.py
Would you like to (E)ncrypt or (D)ecrypt?: E
File to encrypt: subsectionforeigndirectinvestment.csv
Password: test
Done.

Process finished with exit code 0
```

Fig 4.3: Encryption output



```
C:\Users\Shaon\AppData\Local\Programs\Python\Python37-32\python.exe C:/Users/Shaon/Desktop/two/encryption.py
Would you like to (E)ncrypt or (D)ecrypt?: D
File to decrypt: (encrypted)subsectionforeigndirectinvestment.csv
Password: test
Done.

Process finished with exit code 0
```

Fig 4.4: Decryption output

## 4.4 DESCRIPTIVE ANALYSIS

We implement our method in programming python language. The execution time for different packages like 110kb, 210kb, 316kb and 438kb are described below in the graphs. Figure 4.5. And 4.6 show execution time for encryption and decryption.

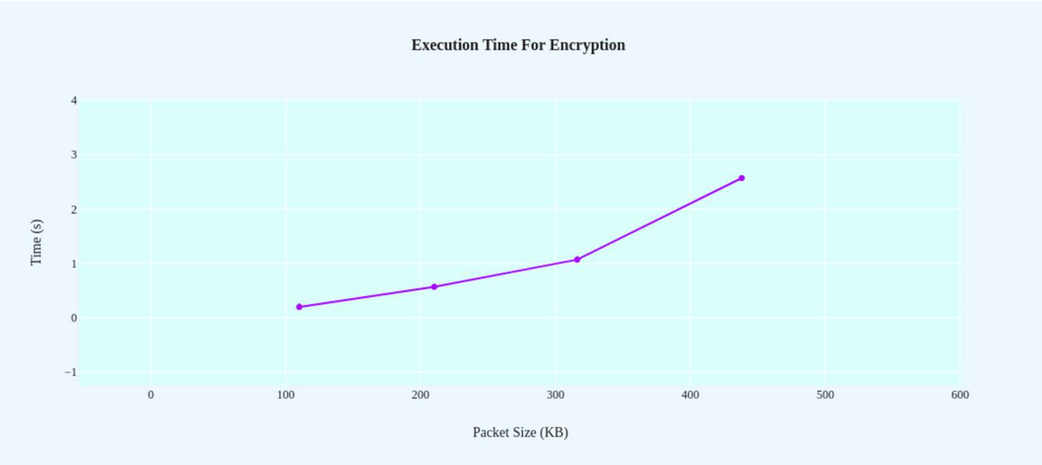


Fig 4.5: Execution Time of Encryption

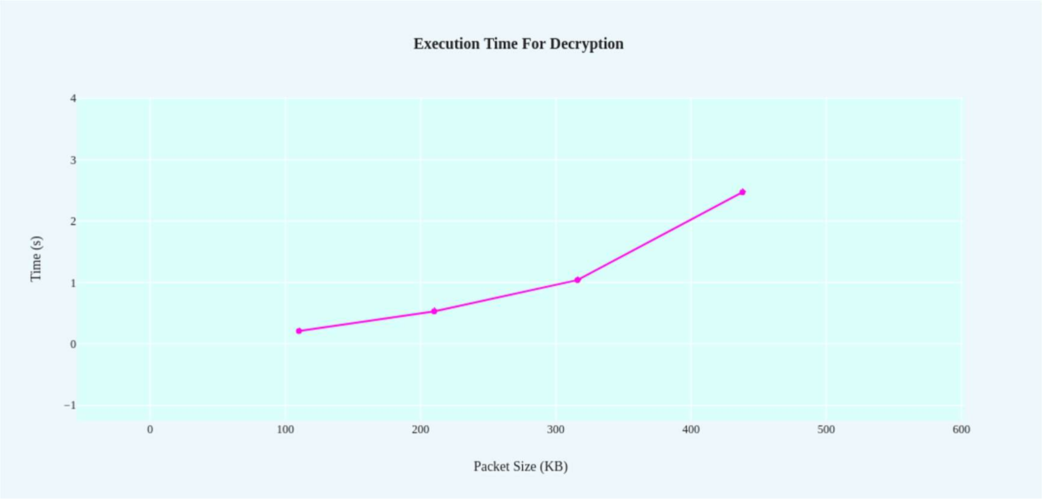


Fig 4.6: Execution Time of Decryption

# CHAPTER 5

# CONCLUTION AND IMPLICATION FOR FUTURE RESEARCH

## 5.1 CONCLUSIONS

Cloud computing is now a demanding technology in this digital world, but there are so many security issues that are the main concern. Many researchers try to solve out the security issues. In this paper, our proposed model will be a success in the case of data security. We provided a secure method for encryption and that will protect the data after uploading in the cloud.

## 5.2 IMPLICATION FOR FUTURE RESEARCH

In the future, we will try to implement our proposed method in user-friendly mood in a web application as well as Android users. After uploading the encrypted file in the cloud the risk became reduce in zero level. In our future work, we will try to make an authentic system for the correct user.

## REFERENCES

[1] W. A. Sultan Aldossary, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 7, no. 4, pp. 485-498, 2016.

[2] D. P. K. V. S. ShankarNayak Bhukya, "Data Security in Cloud computing and Outsourced Databases," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) ,* Vols. 978-1-4673-9939, no. 5, pp. 2458-2462, 2016.

[3] S. K. Mrinal Kanti Sarkar, "A Framework to Ensure Data Storage Security in Cloud Computing," *IEEE,* 2016.

[4] Imperva, "Top 10 Security Concerns for Cloud-Based Services".

[5] S. I. R. K. L. A. A. O. A. S. Raja Mohamed Jabir, "Analysis of cloud computing attacks and countermeasures," 2016.

[6] B. Shereek, "Improve Cloud Computing Security Using RSA Encryption," IOSR Journal of Engineering, vol. 4, no. 2, pp. 1-8, 2014.

[7] M. a. D. D.Vasumathi, "Query based computations on encrypted data through homomorphic encryption in cloud computing security," *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* Vols. 978-1-4673-9939-5, no. 16, pp. 3820-3825, 2016.

[8] H. S. A. a. S. E.-E. Eman M. Mohamed, "Data Security Model for Cloud Computing," *researchgate,* 2013.

[9] R. A. P. Arora, "Secure user data in cloud computing using encryption algorithms," *International Journal of Engineering Research,* vol. 3, pp. 1922-1926, 2013.

[10] D. s. T. Gaura, "A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing," *I.J. Wireless and Microwave Technologies,* vol. 1, pp. 23-33, 2016.

[11] "Tresorit," [Online]. Available: https://tresorit.com/.

[12] B. M. a. K.-K. R. Choo, ", "Cloud storage forensics: own Cloud as a case study," *Digital Investigation,* pp. 287-299, 2013.

[13] "Viivo," [Online]. Available: https://viivo.com.