iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 7 **Issue:** VII **Month of publication:** July 2019

**DOI:** http://doi.org/10.22214/ijraset.2019.7205

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: 7.177*
*Volume 7 Issue VII, July 2019- Available at www.ijraset.com*

# Data Security by Encryption-Decryption using AES Algorithm of Cryptography

Chandani Luhaniwal[1], R. K Vyas[2]
[1]*Student,* [2]*Professor, Department of computer science Engineering, Shekhawati Engineering College, Jhunjhunu*

***Abstract:*** ***Cloud computing describes the employment of an applications, information and infrastructure. It provides a collection of resources and services like computation, network and the data storage are offered in an exceptionally pay as the manner and services. With the widely known implementation of cloud computing various organizations have issues to connect with their knowledge security. The data security is also in the main things that are dealt in the cloud computing environment. Throughout cloud computing distributed resources are shared among the agency of consolidate in expose environment. There are a number of organizations those whole businesses is depends on their data. There are a lots of cases where data is leaked internally by the employees at cloud provider's end that leads to lose the believe in the cloud provider persons and organization has a fear to transfer towards the cloud while in that type of case an organization can leads to complete interruption of their business. In some beforehand works, researchers tried to reduce the data leakage on the cloud through encrypting the data that is at rest. Several encryption algorithms are accustomed to perform these actions. In this thesis work present a solution to reduce the data loss/leakage with the better level compare than others and together with it also provides better protection to them. In this thesis work the encryption technique are used before uploading the information on the cloud. Additionally hashing methods is also used to consult the authenticity of the information after downloading by the cloud. AES algorithm used to give confidentiality whereas SHA hashing algorithm is intended for authenticity of the data. Therefore this work provides us an improved way to encrypt and***
***decrypt the data and also give the facility to confirm the authenticity rather than the previous work.***
***Keywords: Cryptography, Encryption- Decryption, AES algorithm, Hash function.***

## I. INTRODUCTION

Now a day's data security is important for everyone. Many organizations like private and government office having confidential data. They need their data maintain confidential at their work place also [1]. They need a better security for their work place. Some time they are faces data leakage problem. In this thesis focusing on prevent data leakage problem. Most of time data is saving in computers. Online data leakage problem is latest big problem [2] Data loss problem is face when data is removed from computer intentionally or unintentionally. This type of data having both i.e. physically and logically. Organizations needs all the data should be maintain confidential. If their important data leak from their work place then they can face some small or big problem. Any body can leak their organization base data which is backbone of this organization. So data confidentiality is biggest problem of any organization. Now a day we are listening on television news about data leakage of customers. Some data is using by American president election time. Facebook is big company but it facing blame of data leakage. Paytm is a company which is famous payment transfer platform for Indian user. When demonstration announced by our honorable prime minister that time people are interested to use online payment system. i.e. easy for them because of its time saving and cashless method. Paytm is a company which is famous online payment transfer platform for Indian user. That time paytm gives many offers to their consumers so many people connect with this.This company having several important data of their customers. Like their phone number, names, bank details, address. All data is saving in their server system. But a employee of this company using their data to give hackers for fraud. That type of data leakage problems are faced by organization. So they need more security for their data [3]. An organization needs more security for their confidential data. So according to my literature survey DLP (Data Loss/Leakage Prevention) is a computer security method which is used for identify, monitor and protection of data at many stages like use of this data, at motion time of the data and when data at rest[4]. And other survey is cryptography work is done better with AES. The AES (Advanced Encryption Standard) is a Symmetric Block cipher cryptography algorithm. This is used to protect classified information. Throughout the world AES used to encrypt sensitive data in software and hardware [5]. It is easy to implement in software and hardware and it gives good defense against different types of attack techniques. AES algorithm is one of the well-organized algorithms and it is commonly supported and adopted on hardware and software. In this paper, explains the significant features of AES algorithm and presents some earlier researches that have done on it to estimate the performance of AES to encrypt data beneath different parameters.

According to the outcome obtained from researches shows that AES(Advanced Encryption Standard) has the ability to provide much more protection compared to other algorithms similar to DES, 3DES etc[6]. The AES algorithm had to be flexible, publicly defined, free to use, widely use and able to run professionally in both hardware and software. The middle design principle of the AES algorithm is the acceptance of symmetry at different platforms and the good organization of processing [7].

## II. METERIALS AND METHODS

The presented work is shows the encryption and decryption of any PDF file. In this we focus on many aspects also. We need some software's for that and require some study material. The presented work is valuable as

*1)* The work is based on the encryption and decryption. So we need to encrypt and decrypt much better PDF file compare than others.

*2)* In this work we use many PDF files which are made by self using the data of latest news or important details.

And now days this is very important work for organizations and personal use also. So I done my work with help of AES algorithms and its already describe in chapter 1 and chapter 2 after this we use this algorithm in PYTHON 2.7 and use MYSQL connector for database and XAMPP server for local server.

The Work has performed the also analysis with other encryption decryption algorithms.

In our working process first of all this is describes with the help of a simple algorithm so here describe Algorithm for presented work.

*a)* *Step 1:* Login the main page of encryption and decryption.
*b)* *Step 2:* Option form shown.
*c)* *Step 3:* 3 option shown in option form- encryption, decryption and logout.
*d)* *Step 4:* Select encryption option.
*e)* *Step 5:* Write password for encrypting file.
*f)* *Step 6:* File encrypted.
*g)* *Step 7:* Select decryption by option form.
*h)* *Step 8:* Write same password for decrypting file.
*i)* *Step 9:* If password is right then file decrypted otherwise shown error.
*j)* *Step 10:* Select Logout by option form.

The flowchart of the process is as follows

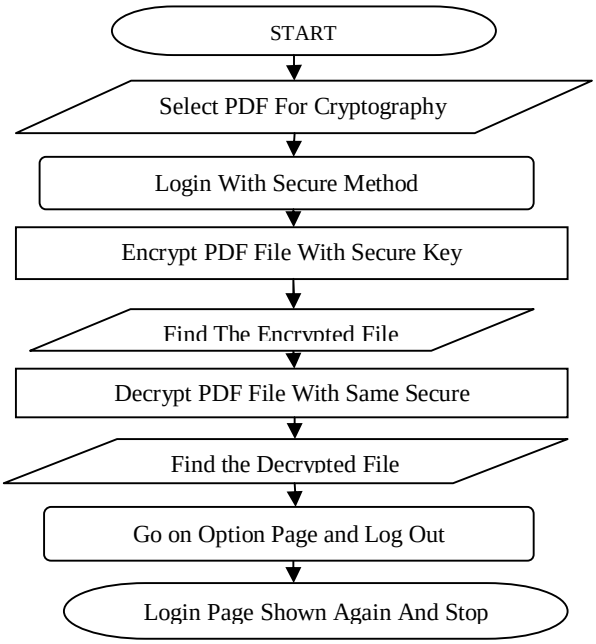



Figure 2.1: Flow chart

Here we use 5 PDF files for practical work those are taken form latest issues or news. Details of PDF files are mention below.

| S. No. | PDF Name | Topic | File Size |
|---|---|---|---|
| 1 | Test 1 | Election pattern | 230 kb |
| 2 | Test 2 | What's with our wheels | 25 kb |
| 3 | Test 3 | Gulf and Af-Pak fast changing | 94 kb |
| 4 | Test 4 | Jair bolsonaro | 630 kb |
| 5 | Test 5 | OPEC and its goals | 69 kb |

Table 2.1:- Used PDF files details for experiment.

## III. IMPLEMENTATION

The entire process of encryption and description takes few steps. We use PYTHON 2.7 for this work. We make it so easy for work. Many encryption method also developed but we make our cryptography method is so easy for user. So it didn't take so many steps. 1 click and you can encrypt your PDF file and after 1 click user can decrypt its PDF file. But the user need same secure key called password for encrypt and decrypt.

Some results also mention below –

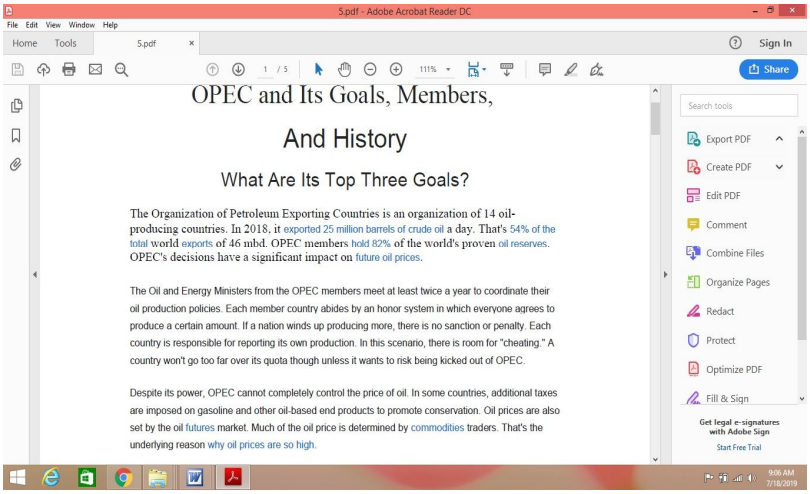



Figure 3.1:- Sample image 1

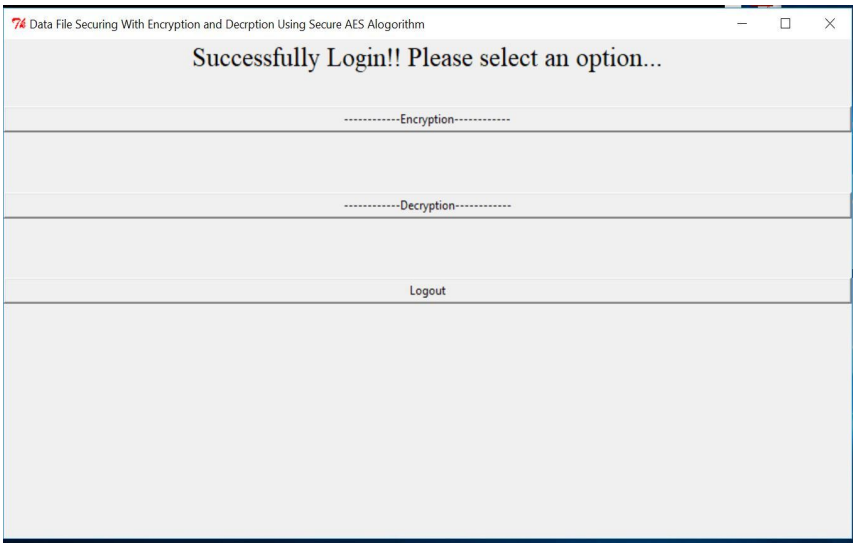



Fig 3.2:- Option form page


Fig 3.3- encrypted file.

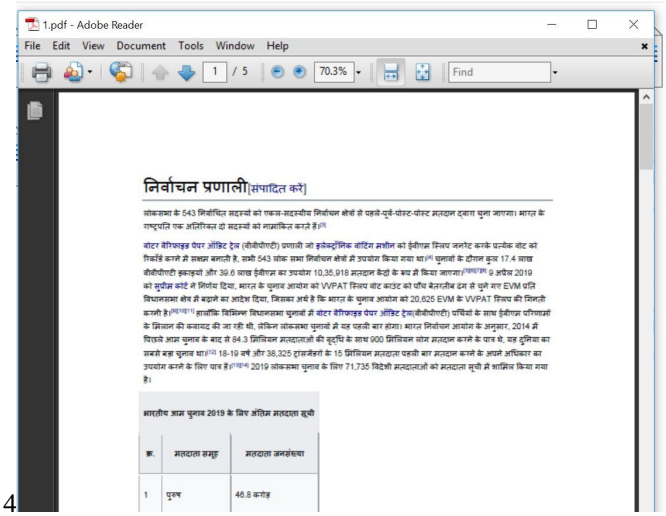



Fig 3.4- Decryption.

## IV. RESULTS

With the help of PYTHON 2.7 and use of AES algorithm we create a code for encryption and decryption. And finally got a encrypted and decrypted file. The final result is mention here for our work.

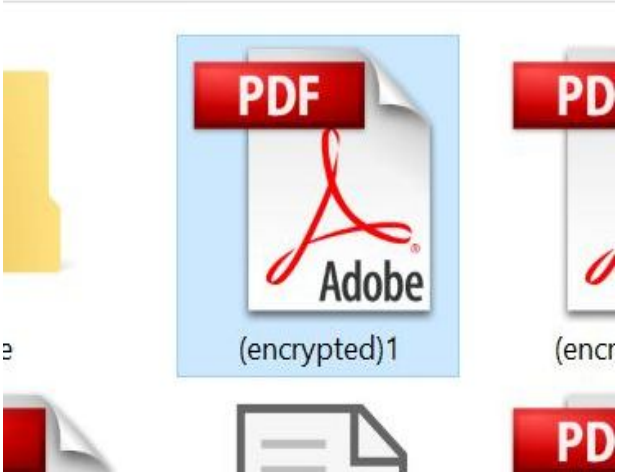



Fig 4.1:- Dialogue box for encrypted file.

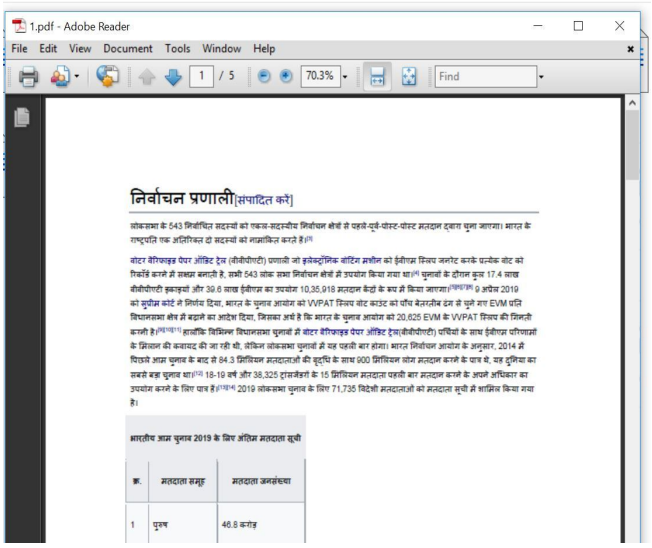



Fig 4.2:- Dialogue Box for Decryption.

Without using secure key any encrypted file cannot open and shown error –

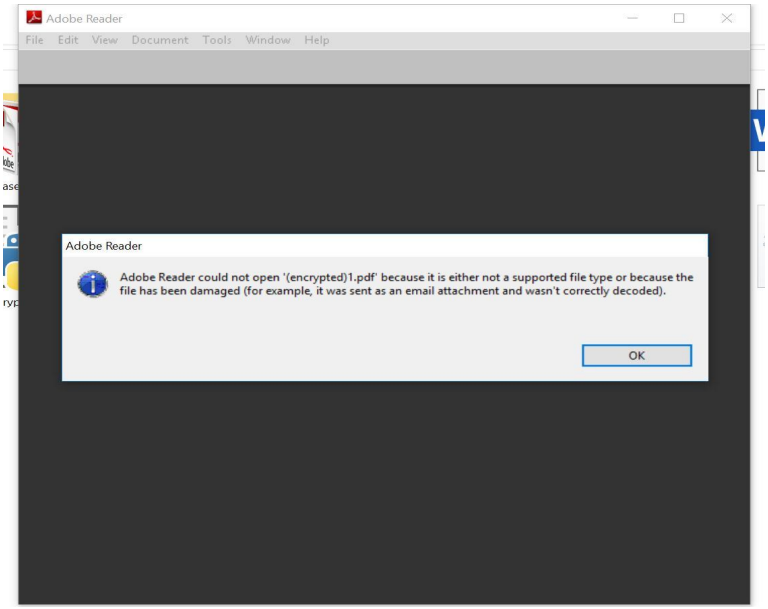



Fig 4.3: When encrypted PDF file open with key

## V. CONCLUSION

Research work is done with the help of AES algorithm of cryptography. We found that in current cryptography AES algorithm is using worldwide and its flexibility reason makes this 'future-proofing'. Till date no realistic cryptanalytic attacks reveled against AES. However, like DES, the AES protection is assured that if algorithm is correctly implemented and excellent key management is employed. I use PYTHON 2.7 for this work and using MYSQL for database and XAMPP server using as a local server.

## VI. FUTURE WORK

Finally the ideas I have proposed that provide their result better but it at some places it also have limitations. In this I am focus only data files but many other data like audio and video also need protection. In future many possibilities to work on encrypt and decrypt the video files also that is little bit hard but requirements are makes it easy. Now a day's many video transfer online and people make video for take them personal. They also need protection with cryptography technology. In future Researchers need to focus on that type of cryptography and makes better algorithms for security of this type of data.

## REFERENCES

[1] Elisa Costante david Fauri ,"A Hybrid Framework for Data Loss Prevention and Detection" © 2016, Elisa Costante. Under license to IEEE. DOI 10.1109/SPW.2016.

[2] Chandramohan.D, Rajaguru.D, Baskaran.R, and Dhavachelvan.P ," A Novel Framework to Prevent Privacy Breach in Cloud Data Storage Area Service" 978-1-4673-2594-3/13/$31.00 ©2013 IEEE

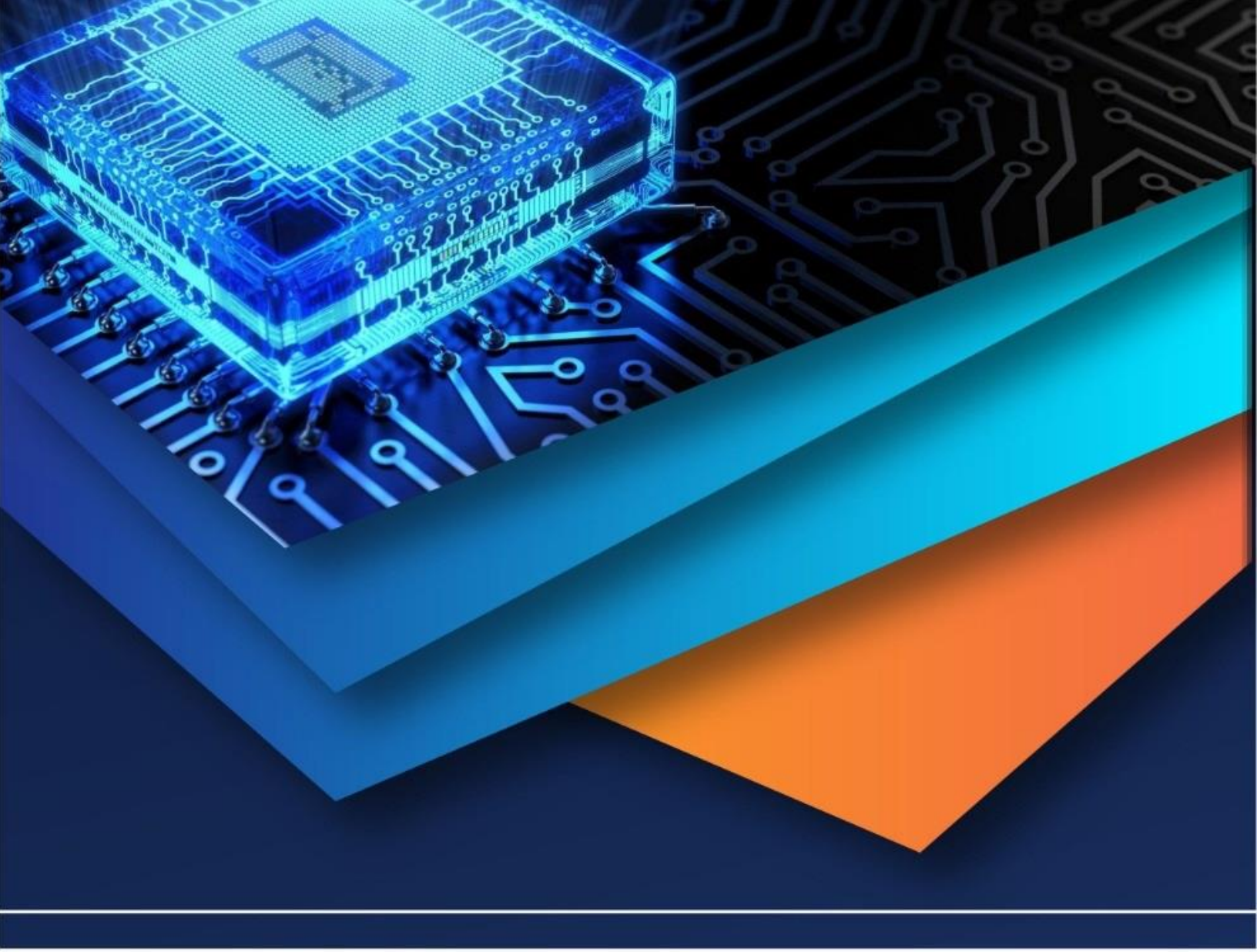
[3] Lance Fiondella, Rehab El-Kharboutly , Swapna S. Gokhale,"Data Loss: An Empirical Analysis in Search of Best Practices for Prevention" 978-1-4799-3766-0/14 $31.00 © 2014 IEEE DOI 10.1109/IC2E.2014.11

[4] Jinhyung Kim , Hyung Jong Kim ,"Design of Internal Information Leakage Detection System Considering the Privacy Violation " 978-1-4244-9807-9/10/$26.00 ©2010 IEEE

[5] Suchita Tayde," File Encryption, Decryption Using AES Algorithm in Android Phone" © 2015, IJARCSSE All Rights Reserved

[6] Ako Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" , Cryptography and Network Security, 2017 Publication Date: June 16, 2017

[7] Aditya Rayarapu, AbhinavSaxena, N.Vamshi Krishna,Diksha Mundhra, "Securing Files Using AES Algorithm" , Aditya Rayarapu et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 433-435



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY