ISSN: 1832-5505

Applied GIS

Vol-10 Issue-04 Oct 2022

# TRI-SEC FOR AWS FILES

S.Manjupriya[1], S.Vinothini[2], P.Mugilarasi[3], A.Gowsalya[4],
Assitance Profrosser[1,2,3,4]
Nadar Saraswathi College of Engineering and Technology,
Theni, Tamilnadu,India.

**Abstract--** The area of cloud security is growing within the field of computer and network security. The cloud platform uses a model of third-party data centers. Platform as a service (PaaS) in the cloud is shown by AWS. It works with a number of computer languages that are used for deploying web applications. Data protection is an important part of cloud computing, and cryptography is used to handle it. TripleDES will be used to secure the file, and the result will be sent to Advanced Encryption Standard (AES). AES is a method for symmetric encryption. It is the safest protection system. For data protection, we use AWS as a cloud server and Tri-protection to keep the files safe. TripleDES and AES cryptography methods can be used to keep data safe, according to the success test.

## I. INTRODUCTION

Cloud computing can be used in a number of different ways, including different systems, services, and software design methods. Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) are some of the service types that can be used with cloud computing. Cloud computing is when you can get computer power, database storage, apps, and other IT tools whenever you need them over the Internet through a site for cloud services. You only pay for what you use.

Amazon Web Services (AWS) is a cloud service from Amazon that gives you services in the form of building blocks. You can use these blocks to make and run any kind of cloud application.These services, or building blocks, are made to work with each other. When they do, you get complex applications that can grow quickly.

Amazon S3 (Simple Storage Service) is a web-based service that lets you back up and archive data and programs online. It is scalable, fast, and cheap. It lets you keep, send, and get any kind of file up to 5 GB in size. People who pay for this service can use the same tools that Amazon uses to run its own websites. The user controls who can see the data, saying whether it is secret or open to everyone.The DES method is used three times in Triple DES, which is a symmetric-key block cipher.

times for every piece of info. Advanced security Standard (AES) is one of the most well-known and safest security algorithms. The block size for AES can range from 64 to 256 bits, and it is a symmetric block cipher.

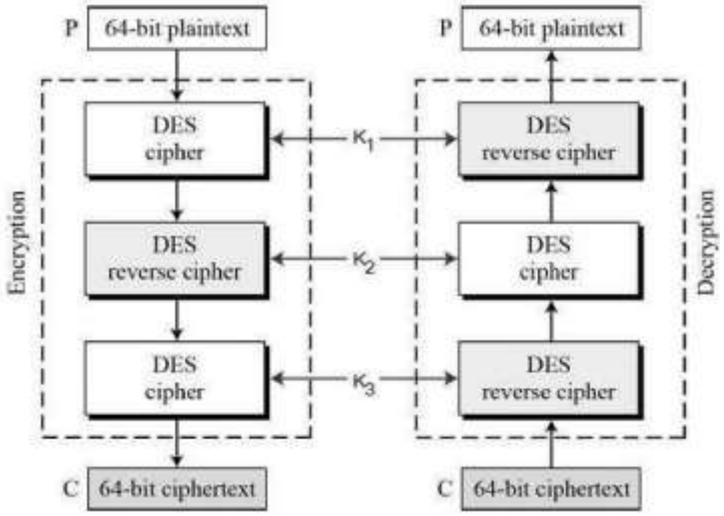
We talk about Tri-Sec for Files using AWS in this paper. We use AWS as a cloud computer tool and then add Triple DES and AES to the website to keep data safe.

## II. SECURITY ALGORITHM

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. TripleDES is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

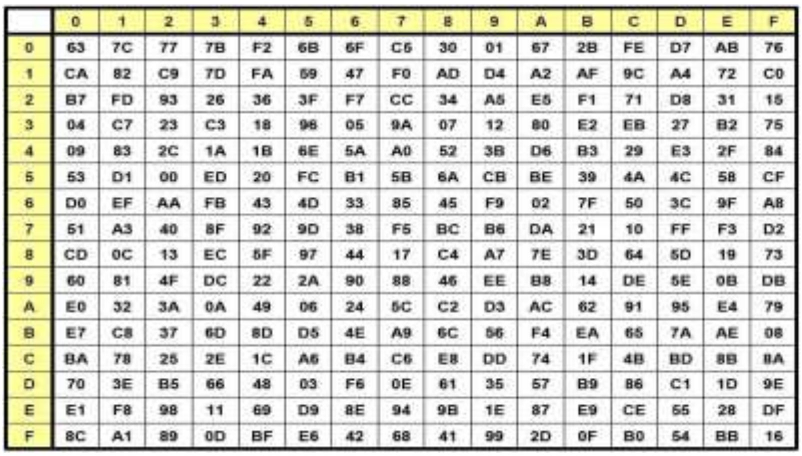
Triple DES expands the size of the key by running the algorithm in succession with three different keys. It makes 48 passes through the algorithm. The resulting key is 168 bits; this can be hard to implement, so there is also a two-key option provided in Triple DES that runs through a method called Encrypt-Decrypt- Encrypt (EDE)

1. Encrypt: The encryption is applied to the content using key 1.
2. Decrypt: This encrypted text is decrypted using key 2.
3. Encrypt: Lastly, the decrypted text from step 2 is encrypted again using key 2.



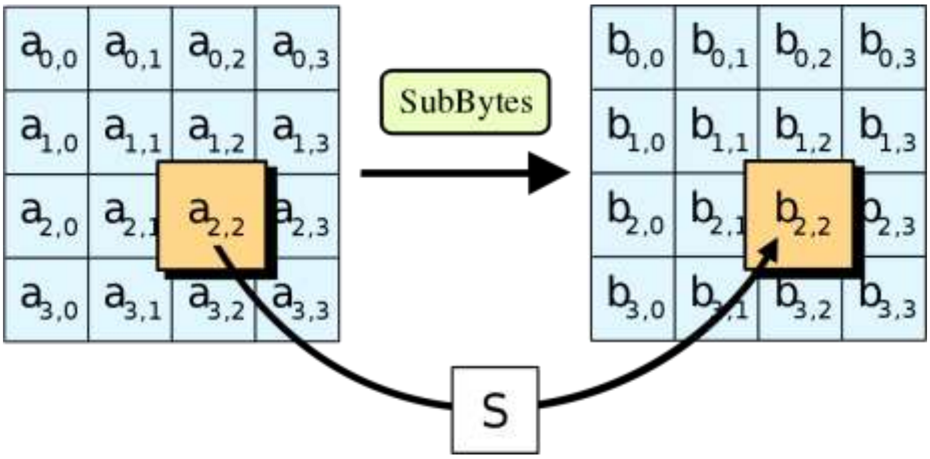
Advanced Encryption Standard (AES) algorithm not only for security but also great speed. AES is the current standard for secret key encryption. AES is a symmetric key algorithm. It is having various ciphers with different keys and the block size. In this plaintext is encrypted with the help of AES and then the cipher text which we have got will again encrypt likewise there will be various round like the AES algorithm includes 10, 12 and 14 round with 128, 192, and 256 key bits. As there are various rounds in this algorithm the plaintext is encrypted many times and this helps the data to have the security.The Advantages It provides strong security from attackers. In this paper, we have focused on AES 128 for making encryption of data.

1. Substitute Bytes In this step, each byte of input data is replaced by another byte from the substitution table (S-box).



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

In the SubByte step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table,


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

2. Shift Rows

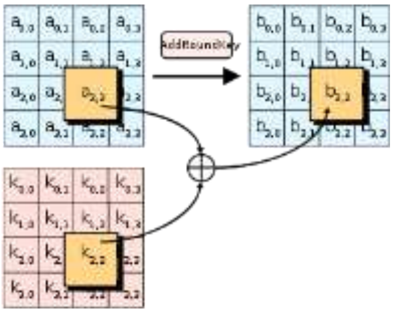
   In the shift Rows, the byte in each row of the state is shifted cyclically to the left. The number of places each byte is shifted differs for each row.

3. Mixing Columns

   In the MixColumns step, each column of the state is multiplied by a fixed polynomial.

4. The AddRoundKey

   In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using XOR operation .

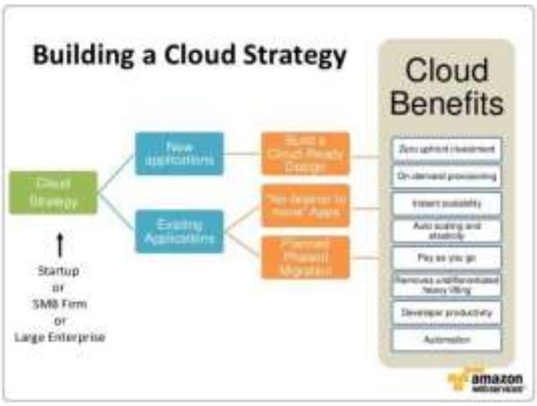


## III. AWS CLOUD

Amazon Web Services (AWS) started to offer IT services to the market in the form of web services, which is nowadays known as cloud computing. With this cloud, we need not plan for servers and other IT infrastructure which takes up much of time in advance. Instead, these services can instantly spin up hundreds or thousands of servers in minutes and deliver results faster. We pay only for what we use with no up-front expenses and no long-term commitments, which makes AWS cost efficient.AWS not only provide resources to develop an application but also helps in deploying the application globally at minimum cost.

AWS provides wide range of cloud computing services that helps in development of a sophisticated application.AWS allows quick development and deployment of an application and hence it allows the team to experiment more frequently.Amazon Web Services provides services from dozens of data centers spread across (AZs) in regions across the world. An AZ represents a location that typically contains multiple physical data centers, while a region is a collection of AZs ingeographic proximity connected by low-latency network links. An AWS customer can spin

up (VMs) and replicate data in different AZs to achieve a highly reliable infrastructure that is resistant to failures of individual servers or an entire data center.



## A. System Requirements

The design of cloud computing architecture should be attractive. It should also allow businesses to quickly access personal resources, and improve public resources without the complexity and time of the installation, purchase, and implementation of traditional physical infrastructure. The architects employed with building a cloud infrastructure, need requirements to be addressed when building their cloud strategy. The requirements of the cloud security which we built are specified below.

Hardware requirements

| | |
|---|---|
| System | Pentium IV 2.4 GHz. |
| Monitor | 15 VGA Color. |
| RAM | 2 Gb. |
| Cloud | AWS |

Software requirements

| | |
|---|---|
| Operating system | Windows. |
| Front End | STS |
| Back End | S3 |
| Cloud | AWS |

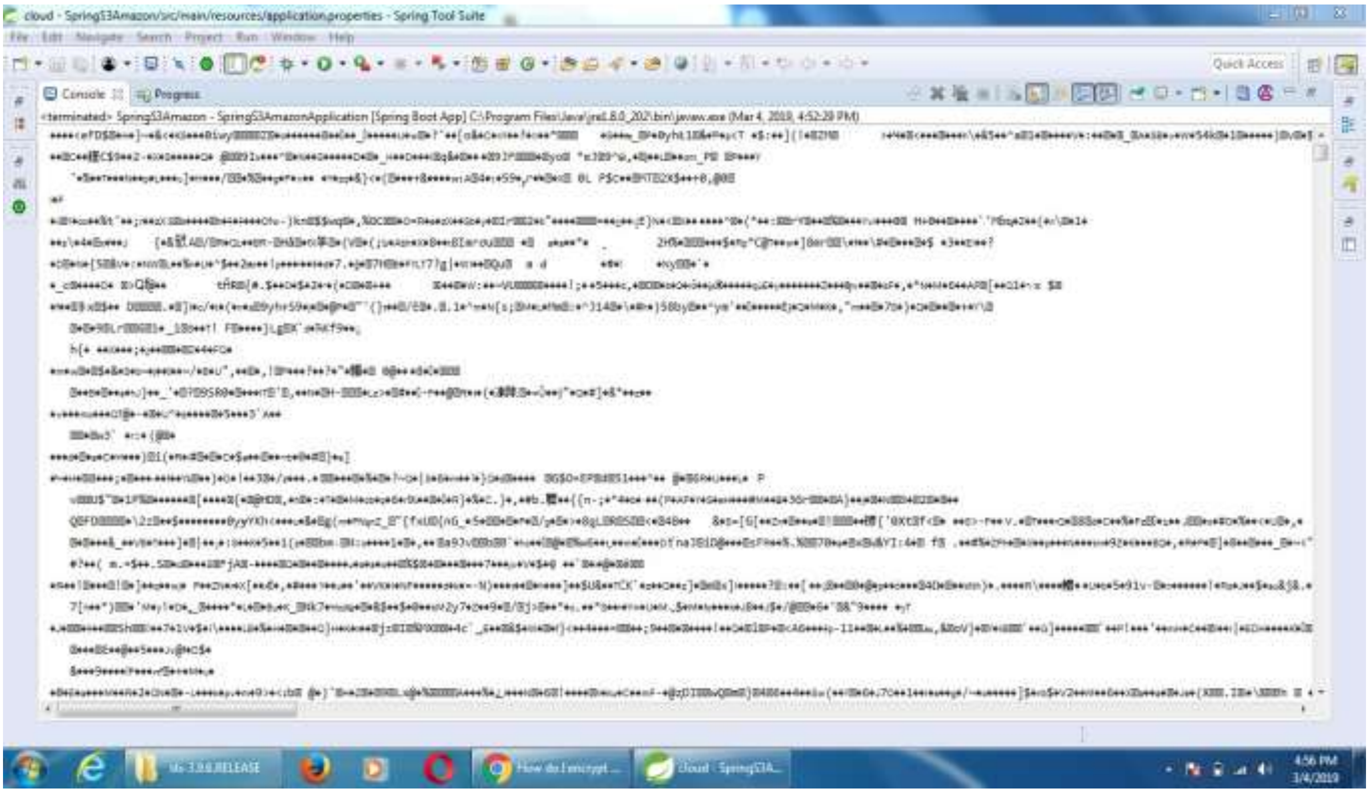
**B. Result**

1. Encrypt & Decrypt File using Triple DES

Firstly, click the button "Encrypt & Decrypt File" and choose the file you want to encrypt in the following format: .jpeg, .doc, .txt,.mp3,.mp4 or .pdf. Then input the key, e.g. 1234, and press the button "Encrypt" to encrypt. To decrypt the file, input the PIN and the decryption key, then press "Decrypt" button.

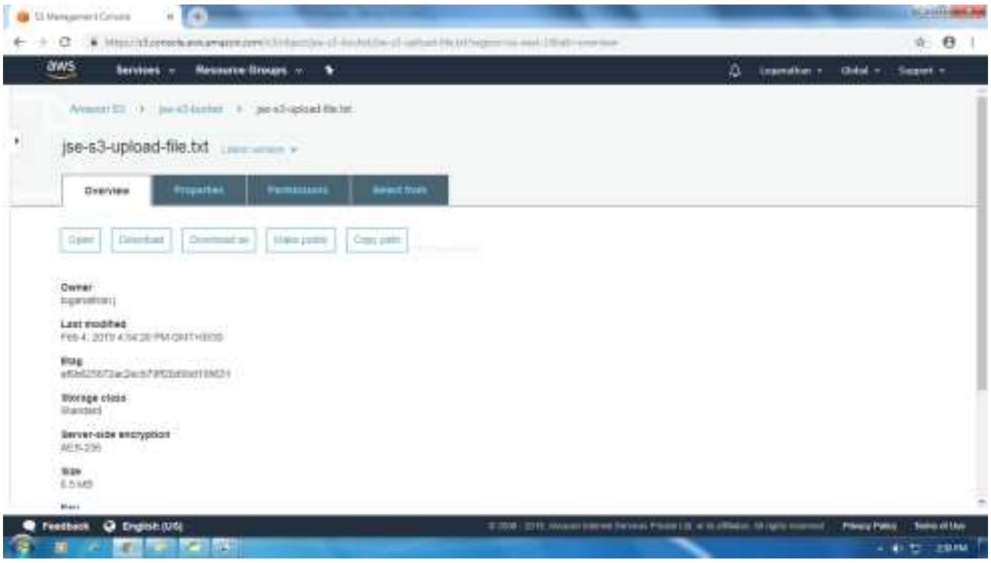
2. AES Encryption and Decryption

After the Triple DES encryption the output given as an input to AES Encryption.The encrypted file will be encrypted using AES in the following format: .jpeg, .doc, .txt,.mp3,.mp4 or .pdf.


cloud - SpringS3Amazon/src/main/resources/application.properties - Spring Tool Suite
File Edit Navigate Search Project Run Window Help
Quick Access
Console
Progress
4:56 PM
3/4/2019

```
<terminated> SpringS3Amazon - SpringS3AmazonApplication [Spring Boot App] C:\Program Files\Java\jre1.8.0_202\bin\javaw.exe (Mar 4, 2019, 4:52:29 PM)
```

h Triple DES and AES encryption the encrypted file will be uploaded in AWS.The encrypted file is protected by AWS.



jse-s3-upload-file.txt

Owner
organation1

Last modified
Feb 4, 2019 4:54:28 PM GMT+0530

Etag
ef6b625873ac2ecb79f2bfd9ef19f621

Storage class
Standard

Server-side encryption
AES-256

Size
6.5 MB

## IV. CONCLUSION

We suggested Tri-Sec for files that use AWS in this paper. There are several steps that need to be taken to set up AWS as a cloud platform. Then, as an application to data security, we set up a website. We use TripleDES and AES as data security algorithms on the page. AES and Triple DES cryptography can be used to keep data safe, as shown by the speed test. Also, figuring out the delay of data encryption shows that the delay time for encrypting data goes up as the size of the data rises.

## REFERENCES

1) D. Meng, “Data security in cloud

computing," in Computer Science & Education (ICCSE), 2013 8th International Conference on, 2013, pp. 810–813.

2) Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data Security in Cloud Computing," in Future Generation

Communication Technologies (FGCT), 2016, pp. 55–59.

3) M. Usman and U. Akram, "Ensuring Data Security by AES for Global Software Development in Cloud

Computing," in IT Convergence and Security (ICITCS), 2014 International Conference on, 2014, pp. 1–7.

4) Babitha.M.P and K. R. R. Babu, "Secure Cloud Storage Using AES Encryption," in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 859– 864.

5) Bih-Hwang Lee, Ervin KusumaDewi, Muhammad FaridWajdi, "Data security in cloud computing using AES under HEROKU", in the 27th Wireless and Optical Communications Conference (WOCC2018).