International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST2182108

Security and Privacy of Sensitive Data in Cloud Computing Using RSA

M. Dhamodaran, Dr. E. Punarselvam, S. Dhinesh Varshan, P. Dinesh Kumar, C. Saravanan, K. Prathap
Department of Information Technology, Muthayammal Engineering College (Autonomous), Tamilnadu, India

ABSTRACT

Article Info
Volume 8, Issue 2
Page Number : 657-661

Publication Issue
March-April-2021

Article History
Accepted : 25 April 2021
Published : 30 April 2021

Today's world internet is being used by almost everyone. Numerous file exchanges take place online including many official documents. These files require some sort of security mechanisms while being transmitted over the Internet. Technology has done a great deal for changing the way we live and do business today. In the fast-moving world we need something essential for fast computation. Along with the popular use of computer, Information security has also become one of the problems which need to be solved. Many security issues like the malware authors, information leakage, endangerment and unauthorized exploitation need to be taken into account. To control those issues, crypto-security is necessary. More Applications started to use Rivest–Shamir–Adleman (RSA). However, Since RSA on large blocks is computationally intensive and largely byte-parallel. System will parallel perform the encryption and decryption process in a distributed environment and the performance analysis shows improvement in terms of execution time and provides the security.

Keywords : Cloud Computing, Security, Advanced Encryption Standards (AES), Rivest–Shamir–Adleman(RSA), Heroku cloud.

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. The idea of cloud computing is based on a very fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption." Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

II. PROPOSED SYSTEM

Cryptography is one of the most notable and desired techniques to protect the data from attackers by using two essential processes. These processes are listed as Encryption and Decryption. Encryption is the process of converting the data to stop it from attackers to read the original data clearly. Encryption involves conversion of plain text to unreadable format. It is known as cipher text. The user cannot read the above format. Hence, the next process that is carried out by the user is Decryption. In the world of computing, there exist security issues for storing the data in cloud. In order to secure data in cloud RSA encryption technique is used in it. RSA is a block cipher with a block length of 128 bits. It permits three differentkey lengths: 256, 192,128 or bits.

III. ALGORITHM

Rivest–Shamir–Adleman (RSA)

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm.Asymmetric means that there are two different Keys. It is also called public key cryptography, because one of the keys can be given to anyone.

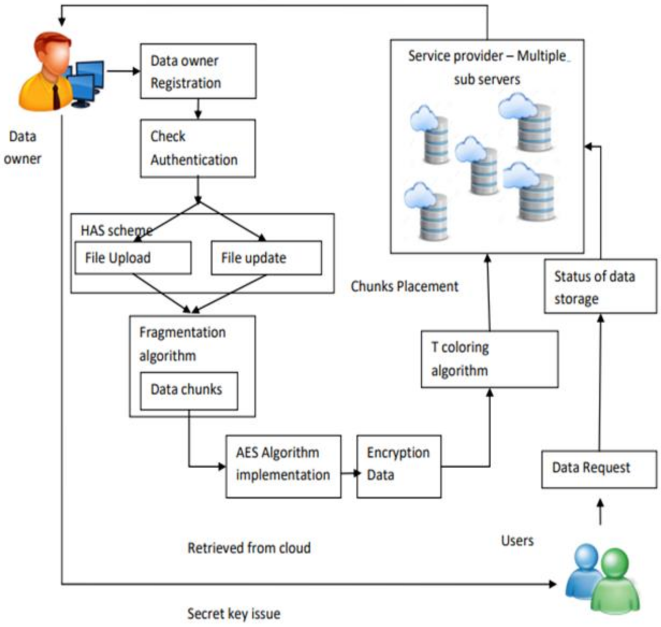


Fig. 1 SYSTEM ARCHITECTURE

IV. MODULES DESCRIPTION

A. Data Owner Module

Data owner has legitimate rights and complete control over a single piece of data or collection of data elements of the cloud. In It module, data owner has the authority to edit, modify, create, share and restrict access to the cloud data. Data owner is the one who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. In it system, the owner of data can access and archive the data stored by the Cloud Service Provider. The data user has to be given authority by data owner to access, manipulate or perform any action on cloud data user sends a key request to data owner and intern to the cloud. File upload section is where the user uploads files either of .txt, .jpg, and .png format. The file then is encrypted using the key generated by RSA algorithm in the cloud administrator module.

B. Data User Module

Data user uses the cloud to store data and access it at any point of time. The data user just wants to use the application software such as MS Office, Paint Brush, and Image Processing Software etc. It sort of service is provided by Software as a Service model of cloud computing which gives freedom to the user from getting license of software Registration module is present for new users to register by providing details such as username and password. Log-in module allows user to log in to one's cloud data segment. The user can search for required files present in the cloud storage. These files are uploaded by the data owner. The request for key can be sent in the key request page of it module. Using the key sent by data owner, the data user can decrypt the file and download it.

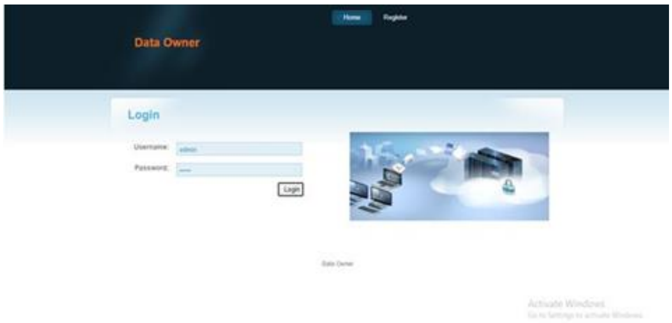
C. Cloud Administrator Module

The cloud administrator module depicts the cloud service providers in the system. There are various cloud service providers which includes Microsoft azure, cisco, Google, Verizon, etc. In It module, cloud administrators have two main responsibilities i.e. It configures the Cloud Management service and it supervises and manages the services. The features of cloud administrator module include the following: The cloud administrators can outlook pending requests for cloud resources it accepts to change requests linked with moderations to cloud resource. It can view and examine the data on cloud resource deployments it supervises key metrics and requests for cloud resources it helps to run Discovery on the cloud resources.

V. IMPLEMETATION

System implementation is the important stage of project when the theoretical design is tuned into practical system. The main stages in the implementation are as follows: Planning, Training, System testing and Changeover Planning. Planning is the first task in the system implementation. Planning means deciding on the method and the time scale to be adopted. At the time of implementation of any system people from different departments and system analysis involve. They are confirmed to practical problem of controlling various activities of people outside their own data processing departments.

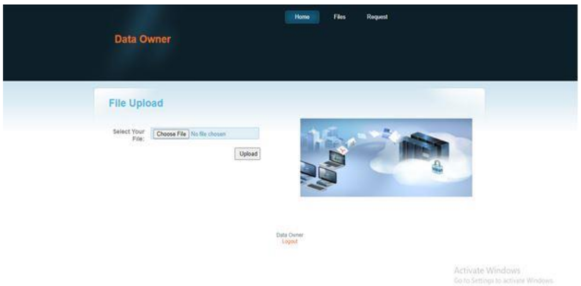
A. Data Owner Module



Username: admin

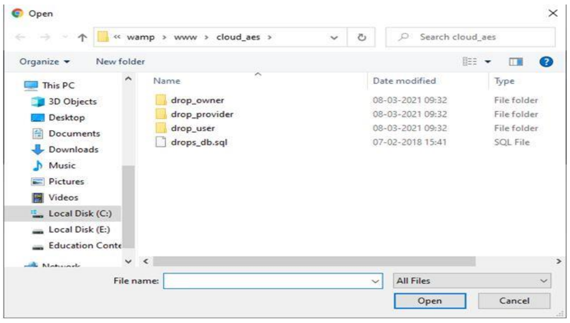
Password: ·····

Fig 2: LOGIN



Select Your File: Choose File No file chosen

Fig 3:FILE UPLOAD

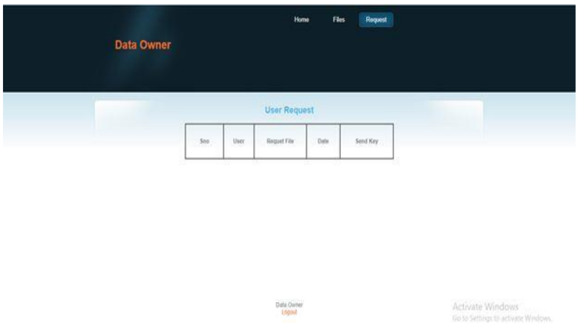


Name	Date modified	Type
drop_owner	08-03-2021 09:32	File folder
drop_provider	08-03-2021 09:32	File folder
drop_user	08-03-2021 09:32	File folder
drops_db.sql	07-02-2018 15:41	SQL File

File name:

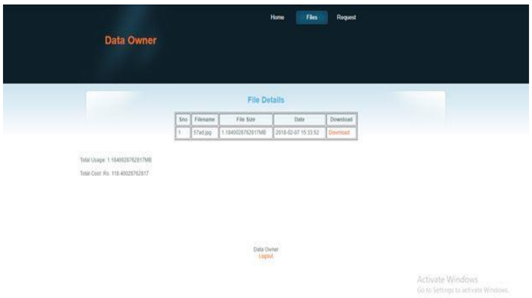
All Files

Fig 4: FILE SEARCH



Sno	User	Requet File	Date	Send Key

Fig 5: FILE STATUS



File Details

Sno	Filename	File Size	Date	Download
1	57ad.jpg	1.1840028762817MB	2018-02-07 15:33:52	Download

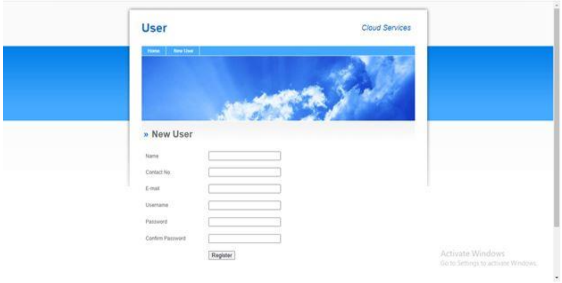
Total Usage: 1.1840028762817MB

Total Cost: Rs. 118.40028762817

Data Owner
Logout

Fig 6: USER REQUEST

B. Data User Module



» New User

Name

Contact No

E-mail

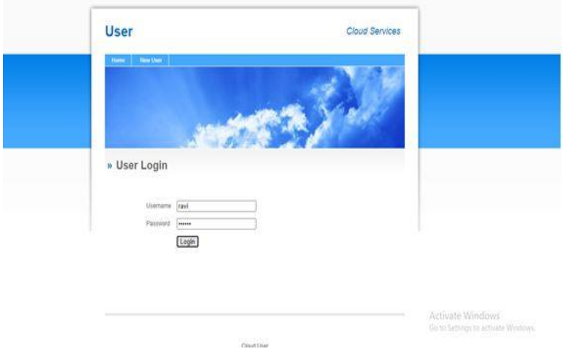
Username

Password

Confirm Password

Register

Fig 7: USER LOGIN



» User Login

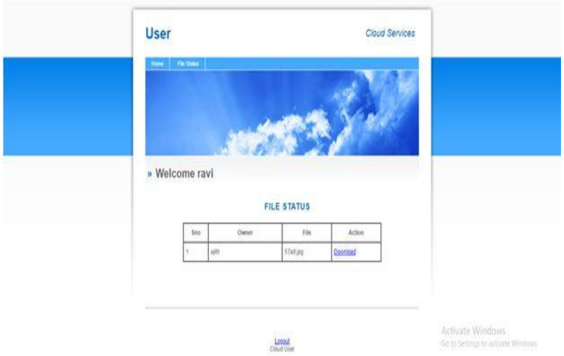
Username ravi

Password ••••••

Login

Cloud User

Fig 8: USER REGISTER



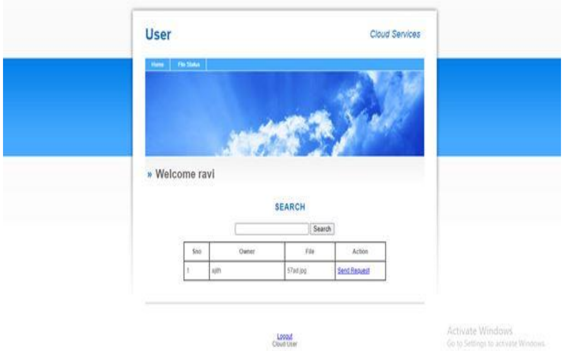
» Welcome ravi

FILE STATUS

Sno	Owner	File	Action
1	ajith	57ad.jpg	Download

Logout
Cloud User

Fig 9:FILE STATUS



» Welcome ravi

SEARCH

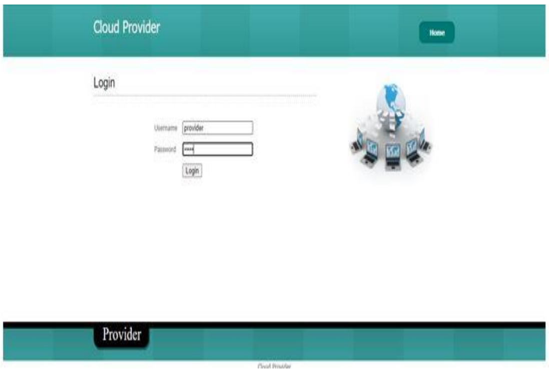
Search

Sno	Owner	File	Action
1	ajith	57ad.jpg	Send Request

Logout
Cloud User

Fig 10: FILE SEARCH

C. Cloud Administrator Module



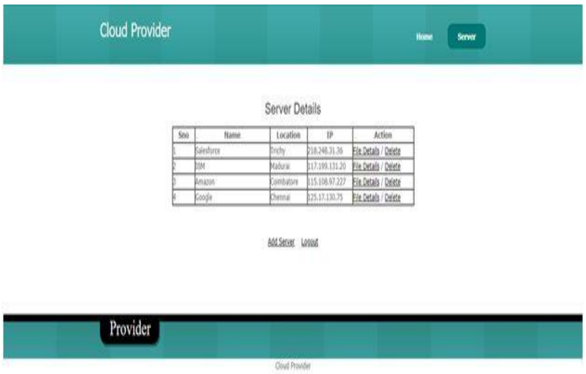
Login

Username provider

Password ••••

Login

Fig 11:CLOUD USER LOGI

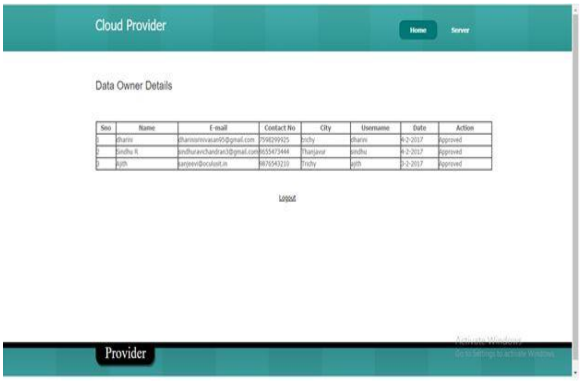


Server Details

Sno	Name	Location	IP	Action
1	Salesforce	Trichy	218.248.31.36	File Details / Delete
2	IBM	Madurai	117.199.131.20	File Details / Delete
3	Amazon	Coimbatore	115.108.97.227	File Details / Delete
4	Google	Chennai	125.17.130.75	File Details / Delete

Add Server Logout

Fig 12: SERVER DETAILS



Data Owner Details

Sno	Name	E-mail	Contact No	City	Username	Date	Action
1	dharini	dharinisrinivasan95@gmail.com	7598299925	trichy	dharini	4-2-2017	Approved
2	Sindhu R	sindhuravichandran3@gmail.com	8655473444	Thanjavur	sindhu	4-2-2017	Approved
3	Ajith	sanjeevi@oculusit.in	9876543210	Trichy	ajith	3-2-2017	Approved

Logout

Fig 13: OWNER DETAILS

VI. CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. Cryptography is one of the most important and prominent skill to secure the data from hackers by using the essential processes that is Encryption and Decryption. RSA encryption is the speedy method that has the flexibility and is easy to implement. Data can also protect against future attacks such as smash attacks. RSA encryption algorithm has high performance and very little storage space without any restrictions while other symmetric algorithms have some restrictions and differences in storage space and performance. The implementation of RIVEST SHAMIR ADLEMAN for securing data bestows benefits of less computation time and less memory consumption in contrast to other algorithms.

VII. FUTURE ENHANCEMENT

Security is an important aspect of cloud computing. The strength of cloudcomputing is the ability to manage risks in particular to security issues. Securityalgorithms can be used for implementing encryption and decryption techniques to securedata.In future, the key length can be expanded using any other key generationalgorithm. The RSA algorithm uses 128 bits. It includes ten rounds or cycles of RSAalgorithm. In future it can be extended to 192 or 256 bits. If 192bit key is used, thenumber of cycles will be 12.

VIII. REFERENCES

[1]. Dr. P.Sivakumar, M. NandhaKumar, R.Jayaraj and A.Sakthi Kumaran, " Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud", Secur. Enhanc. Data Migr. Cloud, vol. 9,no. 23,pp.1-13,2019.

[2]. Cong Wang and Qian Wang," Privacy Preserving and Batch Auditing in Service Cloud Data Storage ", in Future Generation Communication Technologies (FGCT),pp. 55-59,2015.

[3]. L.Kacha and AbdelhafiZitouni," An overview on Data Security in Cloud Computing", Int. J.RecentInnov. Trends Comput. Commum., vol. 5,no.4,pp. 194- 200,2017.

[4]. S.Kumari,Princy,Reema"Security in cloud computing using AES and DES,"Int. J.RecentInnov. Trends Comput. Commun.,vol.5,no.4,pp194-200, 2017.

[5]. D.Meng," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", in IT Convergence and Security(ICITCS),International Conference on, pp.1-7,2013.

[6]. J.R.NSighom,P.Zhang, and L.You,"Secure and efficient privacy preserving public auditing scheme for cloud Storage",Secur. Enhane.DataMigr. Cloud, vol. 9,no.23,pp.1- 13,2017.

[7]. A.Singh,P.Gupta,;R.Lonare,RahulKrSharma,N.A.Ghodichor,"Toward Secure and Dependable Storage in Cloud Coumputing,"Int j.Emerg. Trends Eng.Manag. Res., vol.3,no. 2,pp 1-5,2017.

[8]. Dr.P.Sivakumar, M. NandhaKumar , R.Jayaraj and A.Sakthi Kumaran, " Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud", Secur. Enhanc. Data Migr. Cloud, vol. 9, no. 23, pp.1-13, 2019.

[9]. M.Usman and U.Akram,"A novel Efficient Remote Data Possession Checking Protocol in cloud storage," in IT Convergence and security (ICITCS),2014 International Conference on,pp,1-7,2014.

[10]. D.Zissis and D.Lekkas, "Privacy Preserving in Secure Cloud Data Storage", 2012.

Cite this article as :

"Security and Privacy of Sensitive Data in Cloud Computing Using RSA", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 657-661, March-April 2021. Available at

doi : https://doi.org/10.32628/IJSRST2182108

Journal URL : https://ijsrst.com/IJSRST2182108