IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE DATA TRANSMISSION ON CLOUD COMPUTING USING AES AND ECC ALGORITHM

T. NANCY RANI[1], P. GANESH[2]
1 PG STUDENT 2 PROFESSOR
COMPUTER SCIENCE AND ENGINEERING
SURYA GROUP OF INSTITUTIONS, VIKRAVANDI, TAMILNADU, INDIA

ABSTRACT

Cloud Computing facilitates business by storing an enormous amount of data in the cloud transmitted over the Internet with seamless access to the data and no hardware compatibility limitations. However, data during transmission is vulnerable to man in middle, known plain text, chosen cipher text, related key and pollution attack. Therefore, uploading data on a single cloud may increase the risk of damage to the confidential data. Existing literature study uncovered multiple cryptography techniques such as SA-EDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to secure data storage over multi-cloud. However, existing methods are vulnerable to numerous attacks. This article emphasis on data security issues over multi cloud and proposes a Proficient Security over Distributed Storage (PSDS) method. PSDS divides the data is into two categories; normal and sensitive, furthermore the sensitive data is further divided into two parts. Each part is encrypted and distributed over multi-cloud whereas the normal data is uploaded on a single cloud in encrypted form. At the decryption stage, sensitive data is merged from multi-cloud. The PSDS is tested against multiple attacks and it has been concluded that it is resistant to related key attack, pollution attack, chosen cipher text attack, and known plain text attack. Furthermore, PSDS has less computational time as compared to the STTN and RFD encryption method

Keywords: RFDA, PSDS, Dropbox, Amazon, and Google Drive.

1.INTRODUCTION

Cloud computing environment offers enormous benefits over the local computing environment including financial cost, administrative and management overhead, adaptability, seamless office access, less memory utilization, and so on. Cloud computing provides a platform to users to utilize various assets provided on their request. Cloud computing provides adaptability by giving backup facility like Dropbox, Amazon, and Google Drive. Cloud computing also facilitates clients to cut down their expenses by providing environment for testing applications without building up a physical domain. It also provides administrative facilities, for example, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1], [2]. SaaS offers service to clients, for example, the virtual work area, webmail, and program interface. PaaS provides a stage for using programming language, administrations, libraries, and various apparatuses. IaaS offers online administrations to clients, for example, servers, load balancers, and other computing assets. Due to these reasons today businesses, organization and individual users are moving their data to the cloud. Various models of cloud such as private, public, hybrid and community cloud are defined [3] to provide various services such as infrastructure, software, and others. The security of information with overwhelming size in the cloud is a noteworthy issue. Various strategies have been proposed not only to verify information but also to prevent unauthorized access. An over view of cloud computing and related applications. Data security is a crucial concern while transferring information over the system having various solution proposed in the literature. Be that as it may, cryptography is one of the principal methods used to encipher the data utilizing either symmetric key or asymmetric key. The asymmetric key is considered exceptionally secure as encryption and decryption use different keys. The key generation process of asymmetric key consumes a huge amount of energy and space [4]. Existing proposals have both positives and negatives, for example, Advanced Encryption Standard (AES) is a high- security method used for encryption [5]. Also, Shamir Secret Sharing Scheme is used for encryption [6]. In [7] sensitive data is encrypted by taking XOR with a random number, split and distributed over two clouds.

2. OBJECTIVES

The main objective of this project a multi-valued logic called fuzzy logic is used, which has values of truth and variables ranging. It is used where the meanings of truth vary from absolutely true to utterly false. The fuzzy semantic search based on logic increases the end user's search experience by locating and retrieving the same matching data provided by the user for the corresponding search data. A proficient and secure data storage approach has been proposed that distributes sensitive users' data onto different cloud servers to avoid damage and vulnerability. A mathematical model has been developed and presented along with encryption and decryption algorithms to encrypt and decrypt sensitive as well as normal data.

3. SCOPE

The security of information with overwhelming size in the cloud is a noteworthy issue. Various strategies have been proposed not only to verify information but also to prevent unauthorized access. Cloud computing environment offers enormous benefits over the local computing environment including financial cost, administrative and management overhead, adaptability, seamless office access, less memory utilization, and so on. Cloud computing provides a platform to users to utilize various assets provided on their request. The proposed PSDS algorithm is based on symmetric key encryption to ensure the confidentiality of the data even if the data is uploaded in parts on different clouds. The proposed method uploads sensitive data on multi-cloud in order to protect it from unauthorized access as well as in case of any undesirable situation, all data must not be at a single location

4. LITERATURE SURVEY

[1] P. P. KUMAR, P. S. KUMAR, AND P. J. A. ALPHONSE, ''ATTRIBUTE BASED ENCRYPTION IN CLOUD COMPUTING: A SURVEY, GAP ANALYSIS, AND FUTURE DIRECTIONS,'' J. NETW. COMPUT. APPL., VOL. 108, PP. 37–52, APR. 2018, DOI: 10.1016/ J. JNCA.2018.02.009.

Cloud computing facilitates to store and access the data remotely over the internet. However, storing the data in the untrusted cloud server leads the privacy and access control issues in the cloud. The traditional encryption schemes such as symmetric and asymmetric schemes are not suitable to provide the access control due to lack of flexibility and fine-grained access control. One of the prominent cryptographic technique to provide privacy and fine-grained access control in cloud computing is Attribute Based Encryption. In this paper, we comprehensively survey the various existing key policy and cipher text policy attribute based encryption schemes based on access structure, and multi-authority schemes. Moreover, this review explores more on cipher text policy attribute based encryption in different aspects such as hidden policy, proxy re-encryption, revocation mechanism, and hierarchical attribute based encryption. Further, this paper compares different ABE schemes based on the features, security, and efficiency. This paper also identifies the suitability of attribute-based encryption for practical applications. Finally, this paper analyze the different ABE schemes to find out the research gap and challenges that needs to be investigated further on the Attribute Based Encryption.

[2] A. BOTTA, W. DE DONATO, V. PERSICO, AND A. PESCAPÉ, ‘‘INTEGRATION OF CLOUD COMPUTING AND INTERNET OF THINGS: A SURVEY,’’ FUTURE GENER. COMPUT. SYST., VOL. 56, PP. 684–700, MAR. 2016.

Cloud computing and Internet of Things (IoT) are two very different technologies that are both already part of our life. Their adoption and use are expected to be more and more pervasive, making them important components of the Future Internet. A novel paradigm where Cloud and IoT are merged together is foreseen as disruptive and as an enabler of a large number of app lication scenarios. In this paper, we focus our attention on the integration of Cloud and IoT, which is what we call the CloudIoT paradigm. Many works in literature have surveyed Cloud and IoT separately and, more precisely, their main properties, features, underlying technologies, and open issues. However, to the best of our knowledge, these works lack a detailed analysis of the new CloudIoT paradigm, which involves completely new applications, challenges, and research issues. To bridge this gap, in this paper we provide a literature survey on the integration of Cloud and IoT. Starting by analyzing the basics of both IoT and Cloud Computing, we discuss their complementarity, detailing what is currently driving to their integration. Thanks to the adoption of the CloudIoT paradigm a number of applications are gaining momentum: we provide an up-to-date picture of CloudIoT applications in literature, with a focus on their specific research challenges. These challenges are then analyzed in details to show where the main body of research is currently heading. We also discuss what is already available in terms of platforms–both proprietary and open source–and projects implementing the CloudIoT paradigm. Finally, we identify open issues and future directions in this field, which we expect to play a leading role in the landscape of the Future Internet.

[3] S. RAMGOVIND, M. M. ELOFF, AND E. SMITH, ‘‘THE MANAGEMENT OF SECURITY IN CLOUD COMPUTING,’’ IN PROC. INF. SECUR. SOUTH AFRICA, AUG. 2010, PP. 1–7.

Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. However, the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

[4] S. CHANDRA, B. MANDAL, S. S. ALAM, AND S. BHATTACHARYYA, ‘‘CONTENT BASED DOUBLE ENCRYPTION ALGORITHM USING SYMMETRIC KEY CRYPTOGRAPHY,’’ PROCEDIA COMPUT. SCI., VOL. 57, PP. 1228–1234, JAN. 2015.

With the crucial growth of technology, data security over the network and internet has achieved immense of prominence today and achieving good security is always a talk of a good security method being in place. Therefore, there is need of better security method with better efficiency in order to increase the security and authenticity and to efficiently decrease computational complexity. Although there are many symmetric key algorithms, we proposed a content-based algorithm, which follows the Symmetric key cryptography method. This is an algorithm implementing binary addition operation, a circular bit shifting operation and folding method and as symmetric key cryptography needs the transmission of the secret key along with the ciphered text through the network, a deep concern has given to make the key secure.

[5] R. F. OLANREWAJU, B. U. I. KHAN, A. BABA, R. N. MIR, AND S. A. LONE, ‘‘RFDA: RELIABLE FRAMEWORK FOR DATA ADMINISTRATION BASED ON SPLIT-MERGE POLICY,’’ IN PROC. SAI COMPUT. CONF. (SAI), JUL. 2016, PP. 545–552.

Emerging technologies in cloud environment have not only increased its use but also posed some severe issues. These issues can cause considerable harm not only to data storage but also to the large amount of data in distributed file structure which are being used in collaborative sharing. The data sharing technique in the cloud is prone to many flaws and is easily attacked. The conventional cryptographic mechanism is not robust enough to provide a secure authentication. In this paper, we overcome this issue with our proposed Reliable Framework for Data Administration (RFDA) using split-merge policy, developed to enhance data security. The proposed RFDA performs splitting of data in a unique manner using 128 AES encryption key. Different slots of the encrypted key are placed in different places of rack servers of different cloud zones. The effectiveness and efficiency of the proposed system are analyzed using comparative analysis from which it is seen that the proposed system has outperformed the existing and conventional security standard.

5. SYSTEM ANALYSIS

5.1 EXISTING SYSTEM

Cloud computing environment offers enormous benefits over the local computing environment including financial cost, administrative and management overhead, adaptability, seamless office access, less memory utilization, and so on. Cloud computing provides a platform to users to utilize various assets provided on their request. Therefore, uploading data on a single cloud may increase the risk of damage to the confidential data. Existing literature study uncovered multiple cryptography techniques such as SA-EDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to secure data storage over multi-cloud. However, existing methods are vulnerable to numerous attacks. This article emphasis on data security issues over multi cloud and proposes a Proficient Security over Distributed Storage (PSDS) method. PSDS divides the data is into two categories; normal and sensitive, furthermore the sensitive data is further divided into two parts.

5.2 PROPOSED SYSTEM

The general contributions of this article are: A proficient and secure data storage approach has been proposed that distributes sensitive users' data onto different cloud servers to avoid damage and vulnerability. A mathematical model has been developed and presented along with encryption and decryption algorithms to encrypt and decrypt sensitive as well as normal data. The proposed technique has been analyzed for security against various known attack to assess its security. The proposed technique has also been analyzed for computation and communication overhead in case of both sensitive as well as normal data to assess its complexity. A comparative analysis of the proposed technique has been presented with AES, STRRNS, RFDA, and SA-DES in terms of computation time both for sensitive data as well as the overall encryption/decryption time.

6.SYSTEM DESIGN

6.1 ARCHITECTURE DIAGRAM

The system architecture of the proposed approach for file distribution over multi-cloud. The system architecture consists of user and cloud storage. A data owner is a person who owns data files and a data owner must Login to upload or download a file over the network. After a successful Login, a data owner may decide the file type. Cloud storage is a database that provides a storage place to the users to store their file(s). Different cloud providers have different policies. An application interface (API) is provided by cloud service providers enabling users to interact with its services. The security of information with overwhelming size in the cloud is a noteworthy issue. Various strategies have been proposed not only to verify information but also to prevent unauthorized access. An over view of cloud computing and related applications. Data security is a crucial concern while transferring information over the system having various solution proposed in the literature. Be that as it may, cryptography is one of the principal methods used to encipher the data utilizing either symmetric key or asymmetric key. The asymmetric key is considered exceptionally secure as encryption and decryption use different keys. The key generation process of asymmetric key consumes a huge amount of energy and space.

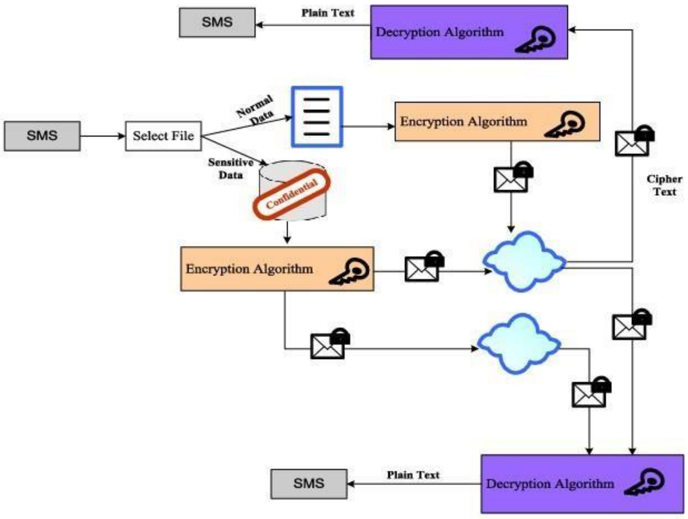


FIGURE 7. Overview of the proposed PSDS

This article proposes a symmetric key based cryptographic method named Proficient Security over Distributed Storage (PSDS) to secure client's information over the cloud. The client chooses whether the information is private (sensitive) or typical (normal) information. The private information is split into two sections, part1 and part2 as appears. After splitting data, encryption steps of PSDS are applied to both parts. Both encrypted parts are uploaded on to two separate clouds, cloud 1 and cloud 2 in order to prevent loss or exposure of data. In the decryption phase, sensitive data from both clouds is downloaded and then merged both parts. After merging apply the decryption method of PSDS to convert cipher text into plain text. In the decryption process of normal data, the data is downloaded from a single cloud and then decryption is applied to transform cipher text to original text.

6.2 ALGORITHM

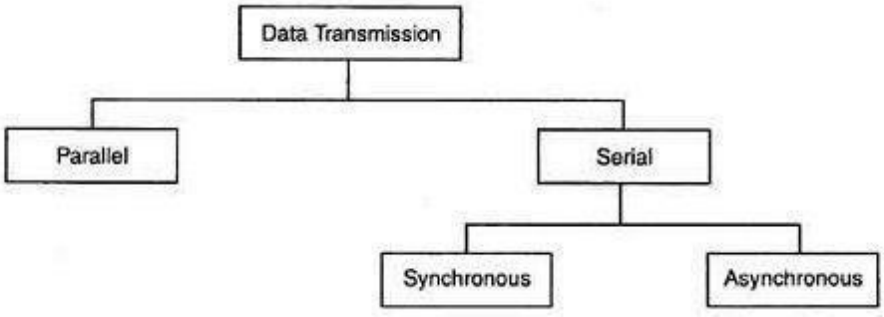
The working of the proposed PSDS approach may be divided into different parts including; Key Generation – to generate keys for symmetric encryption to ensure the confidentiality of the data to be stored on the cloud, a splitting algorithm to divide the sensitive data into parts, and encryption and decryption algorithms to encrypt data while uploading and decrypt it back the owner wants to access the data. It can be used as a parameter to gauge computation efficiency of a particular encryption algorithm. Similarly, to check the performance of the proposed PSDS approach, its encryption time both in case of normal as well as sensitive data has been computed. Figure 9 shows encryption time in milliseconds (MS) of PSDS in case of normal data. The input data is considered byte by byte.

7. SYSTEM IMPLEMENTATION

7.1 LIST OF MODULES

7.1.1 DATA TRANSMISSION

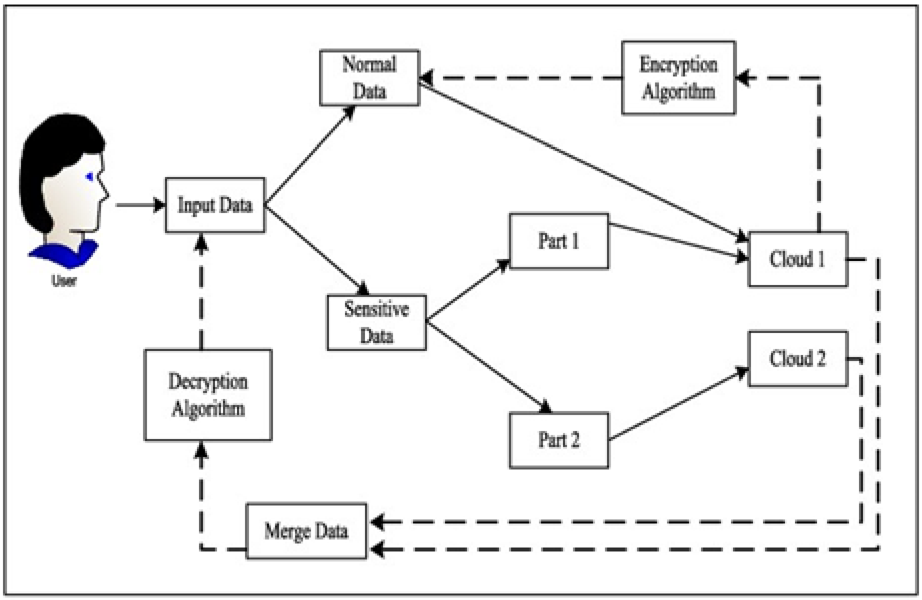
The PSDS is tested against multiple attacks and it has been concluded that it is resistant to related key attack, pollution attack, chosen cipher text attack, and known plain text attack. Furthermore, PSDS has less computational time as compared to the STTN and RFD encryption method.



Cloud computing provides a platform to users to utilize various assets provided on their request. Cloud computing provides adaptability by giving backup facility like Dropbox, Amazon, and Google Drive. Cloud computing also facilitates clients to cut down their expenses by providing environment for testing applications without building up a physical domain.

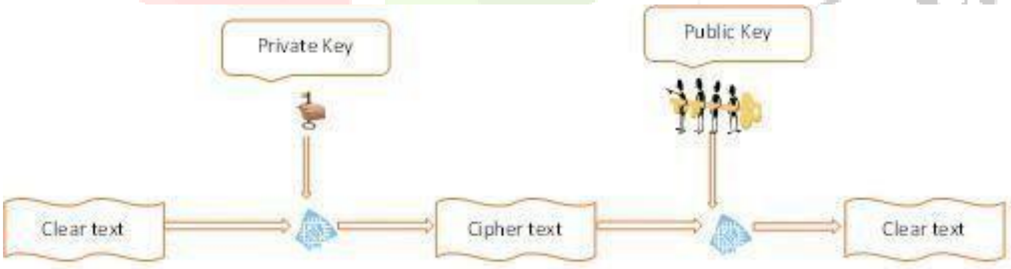
7.1.2 SECURITY

The security of information with overwhelming size in the cloud is a noteworthy issue. Various strategies have been proposed not only to verify information but also to prevent unauthorized access. An over view of cloud computing and related applications is given. Data security is a crucial concern while transferring information over the system having various solution proposed in the literature. Be that as it may, cryptography is one of the principal methods used to encipher the data utilizing either symmetric key or asymmetric key.



7.1.3. CRYPTOGRAPHIC SOLUTION

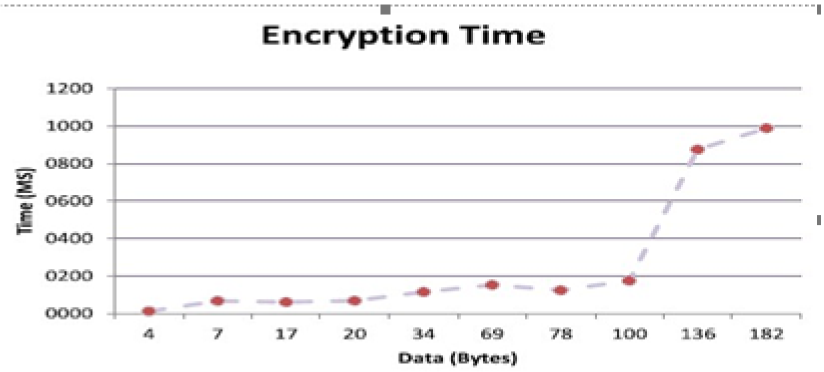
PSDS is an adaptable approach as it is designed to achieve high security by splitting sensitive data on a multi-cloud mechanism. The proposed approach resists against different attacks such as Chosen Cipher text attack, related key Attack, and pollution attack. It also protects data against illegal access by the cloud service providers.



It is used where the meanings of truth vary from absolutely true to utterly false. The fuzzy semantic search based on logic increases the end user's search experience by locating and retrieving the same matching data provided by the user for the corresponding search data. In addition, the model uses semitone similarities to discover the closest related matches, in situations where the exact matches are not usable

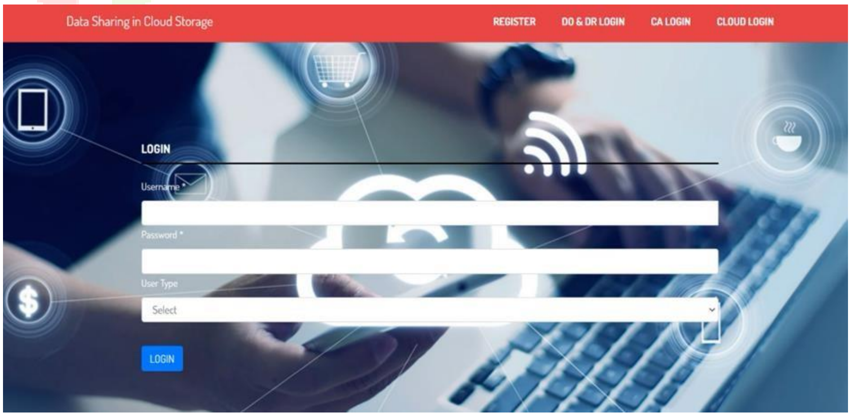
8. RESULTS AND DISCUSSION

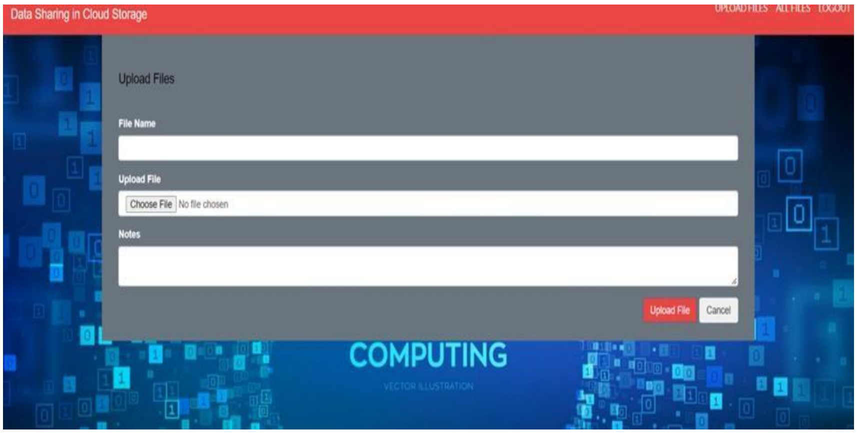
The computational time is an important performance parameter for an encryption approach that shows how many times a certain operation is performed and what is the total number of operations performed during one transactions of a protocol. Computational time is the total amount of time taken by an algorithm to complete a specific amount of computation. the time taken by key generation process, Encryption time and decryption time for different lengths of data. Computational time. The total computational time for 15 bytes is 0089 Ms. It can be seen from the table that for 21 bytes, the computational time is 0120 MS whereas the total computational time for 5 bytes is 0050 Ms.



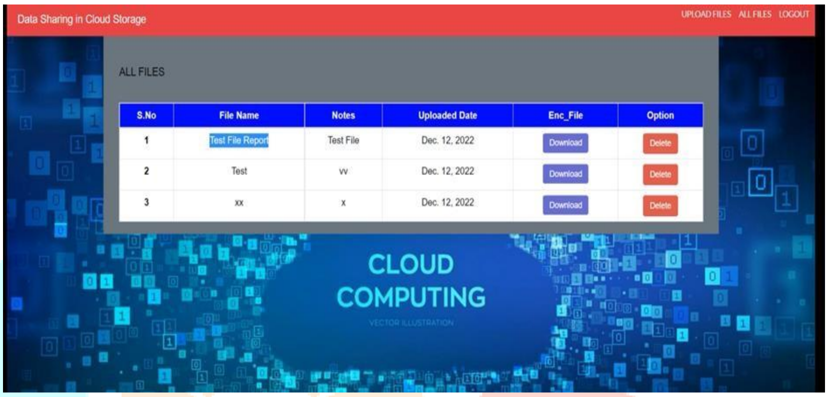
This report contains analyses and discussions of significant problems relating to supervised and unsupervised machine learning methods, outlining the benefits and disadvantages of each algorithm, and addressing the scientific findings analysis. Data Veracity for Cloud Storage through Dual Protection (DVCSDP) gives double security proposed by Kannan. In the initial step, the record is part into various lumps and dispersed over various servers [43]. Suwansrikham Proposed Asymmetric Secure Storage Scheme (ASSS) [44]. In ASSS information proprietor parts the document and approved the client by producing the token which contains the username, secret word, and area. As technology is increasing very rapidly, the number of data raises terrifically. Cloud computing becomes common among people, as people can easily save their huge amount of data in order to save memory consumption. The major issue in storing data on clouds is data security. There is a need to transfer data into cipher text. Multiple approaches are used to secure data over the cloud. Computational time is focused on data security approaches. A complex algorithm is not suitable for data security due to their increasing computational time. The less complex algorithm has security issues. In this paper, we propose PSDS in order to solve the issue. In this paper, we propose PSDS in order to solve the issue. We divide the data in normal and sensitive part. Normal data is encrypted and uploaded over a single cloud while sensitive data is divided into two parts, then encryption steps are applied on these two halves and uploaded on separate clouds. At the time of downloading, these two separate halves are merged and the decryption algorithm is applied in order to obtain plain text. The proposed approach is secure against chosen cipher text, known the plain text, related-key attack, pollution attack, and main-in middle attack.

9. SCREEN SHOTS

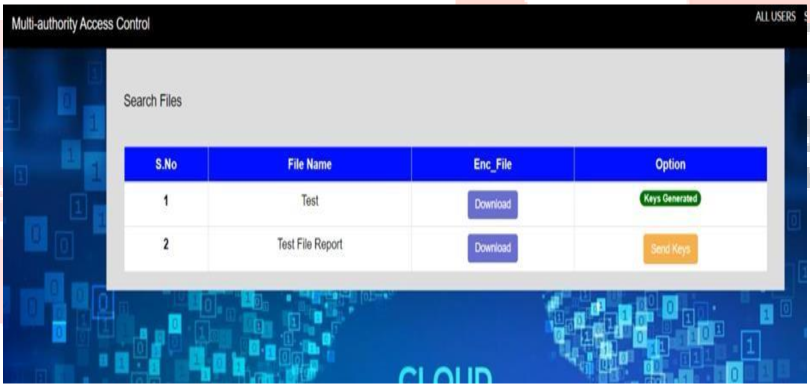




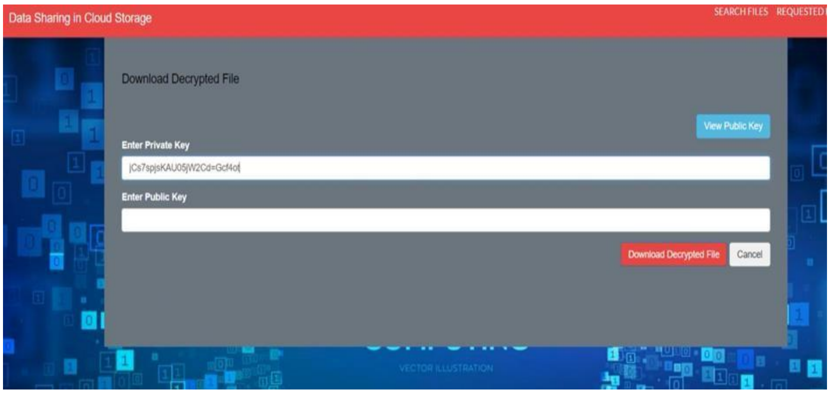
No file chosen



S.No	File Name	Notes	Uploaded Date	Enc_File	Option
1	Test File Report	Test File	Dec. 12, 2022	Download	Delete
2	Test	vv	Dec. 12, 2022	Download	Delete
3	xx	x	Dec. 12, 2022	Download	Delete



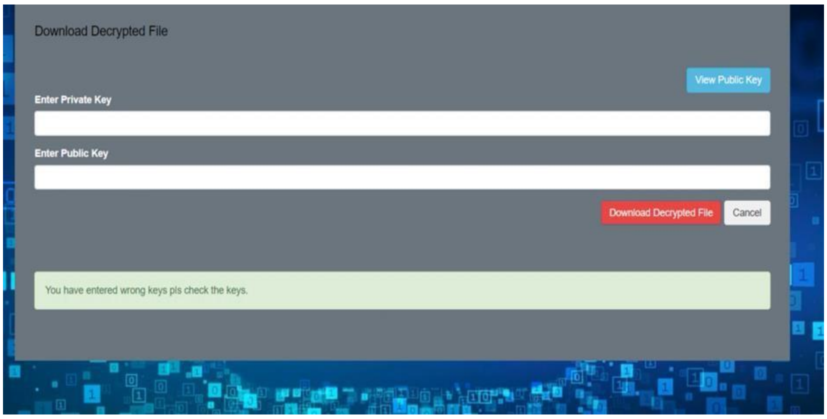
S.No	File Name	Enc_File	Option
1	Test	Download	Keys Generated
2	Test File Report	Download	Send Keys



Enter Private Key

jCs7spjsKAU05jW2Cd=Gcf4ot

Enter Public Key

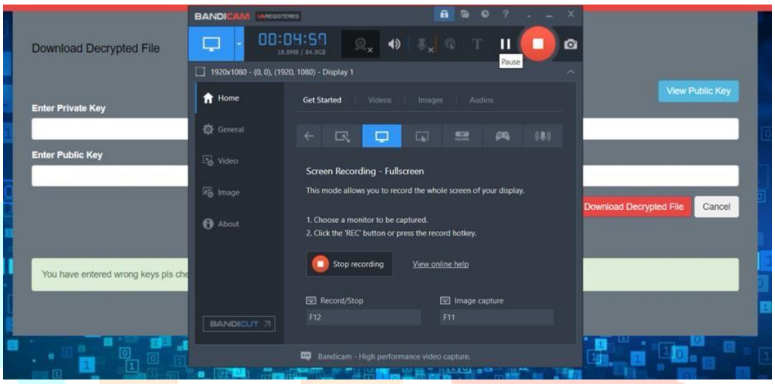


Download Decrypted File

Enter Private Key

Enter Public Key

You have entered wrong keys pls check the keys.



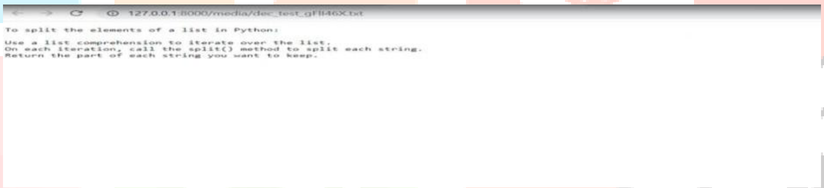
Download Decrypted File

Enter Private Key

Enter Public Key

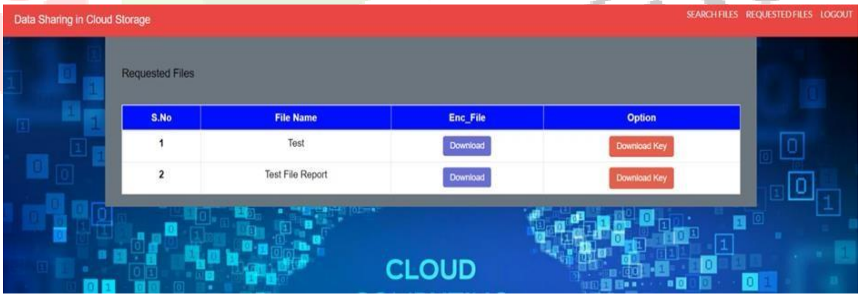
You have entered wrong keys pls che

BANDICAM UNREGISTERED
00:04:57
Pause
1920x1080 - (0, 0), (1920, 1080) - Display 1
Home
General
Video
Image
About
Get Started
Videos
Images
Audios
Screen Recording - Fullscreen
This mode allows you to record the whole screen of your display.
1. Choose a monitor to be captured.
2. Click the 'REC' button or press the record hotkey.
Stop recording
View online help
Record/Stop
F12
Image capture
F11
BANDICUT
Bandicam - High performance video capture.
View Public Key
Download Decrypted File
Cancel



127.0.0.1:8000/media/dec_test_gFlI46X.txt

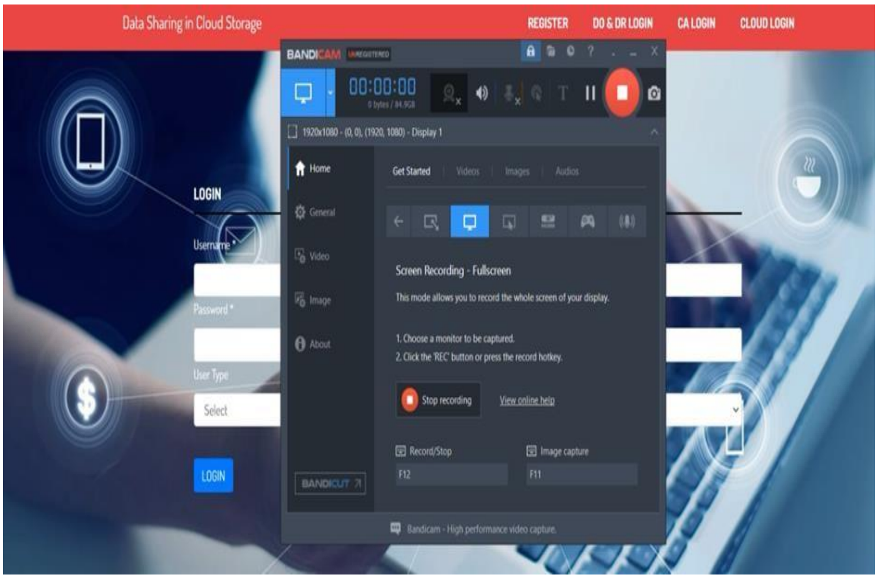
```
To split the elements of a list in Python:

Use a list comprehension to iterate over the list.
On each iteration, call the split() method to split each string.
Return the part of each string you want to keep.
```



Data Sharing in Cloud Storage

Requested Files

S.No	File Name	Enc_File	Option
1	Test	Download	Download Key
2	Test File Report	Download	Download Key



Screen Recording - Fullscreen

This mode allows you to record the whole screen of your display.

1. Choose a monitor to be captured.
2. Click the 'REC' button or press the record hotkey.

10. REFERENCES

[1] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, ‘‘Attribute based encryption in cloud computing: A survey, gap analysis, and future directions,’’ J. Netw. Comput. Appl., vol. 108, pp. 37–52, Apr. 2018, doi: 10.1016/ j. jnca.2018.02.009.

[2] A. Botta, W. de Donato, V. Persico, and A. Pescapé, ‘‘Integration of cloud computing and Internet of Things: A survey,’’ Future Gener. Comput. Syst., vol. 56, pp. 684–700, Mar. 2016.

[3] S. Ramgovind, M. M. Eloff, and E. Smith, ‘‘The management of security in cloud computing,’’ in Proc. Inf. Secur. South Africa, Aug. 2010, pp. 1–7.

[4] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, ‘‘Content based double encryption algorithm using symmetric key cryptography,’’ ProcediaComput. Sci., vol. 57, pp. 1228–1234, Jan. 2015.

[5] R. F. Olanrewaju, B. U. I. Khan, A. Baba, R. N. Mir, and S. A. Lone, ‘‘RFDA: Reliable framework for data administration based on split-merge policy,’’ in Proc. SAI Comput. Conf. (SAI), Jul. 2016, pp. 545–552.

[6] D. P. Yellamma, D. B. C. Narasimham, and M. T. Kumar, ‘‘Cloud computing security using secret sharing algorithm over singleton multi-clouds,’’ Latest Res. Eng. Manag., vol. 1, pp. 1–6, Apr. 2016.

[7] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, ‘‘Intelligent cryptography approach for secure distributed big data storage in cloud computing,’’ Inf. Sci., vol. 387, pp. 103–115, May 2017.

[8] B. S. Rawal, V. Vijayakumar, G. Manogaran, R. Varatharajan, and N. Chilamkurti, ‘‘Secure disintegration protocol for privacy preserving cloud storage,’’ Wireless Pers. Commun., vol. 103, no. 2, pp. 1161–1177, Nov. 2018.

[9] O. Zibouh, A. Dalli, and H. Drissi, ‘‘Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach,’’ J. Theor. Appl. Inf. Technol., vol. 87, no. 2, pp. 300–307, 2016.

[10] K. Subramanian and F. L. John, ‘‘Secure and reliable unstructured data sharing in multi-cloud storage using the hybrid crypto system,’’ Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 6, pp. 196–206, 2017.