JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# A Secure Data Transmission Framework for Cloud Environments: AES and ECC

**Maddineni Venkateswarlu[1] ,Dr N Subramanyam[2]**
[1]Research Scholar, [2]professor,Department of Computer Science and Engineering ,Annamalai University, Tamil nadu , India.

ABSTRACT

Cloud Computing facilitates commercial enterprise through storing an widespread amount of statistics within the cloud transmitted over the Internet with seamless get right of entry to to the data and no hardware compatibility barriers.However, information all through transmission is liable to man in center, recognised simple textual content, chosen cipher textual content,related key and pollutants assault. Therefore, importing statistics on a unmarried cloud may additionally growth the risk of harm to the confidential facts. Existing literature examine exposed multiple cryptography strategie such as SA-EDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to comfortable statistics storage over multi-cloud. However, current methods are liable to
numerous attacks. This article emphasis on statistics protection problems over multi cloud and proposes a Proficient Security over Distributed Storage (PSDS) technique. PSDS divides the information is into classes; everyday and touchy, furthermore the touchy data is in addition divided into elements. Each component is encrypted and disbursed over multi-cloud while the normal statistics is uploaded on a single cloud in encrypted shape. At
the decryption level, sensitive data is merged from multi-cloud. The PSDS is examined towards more than one assaults and it has been concluded that it is immune to associated key attack, pollution attack, selected cipher textual content assault, and regarded plain textual content assault. Furthermore, PSDS has much less computational time as compared to the STTN and RFD encryption technique
Keywords: RFDA, PSDS, Dropbox, Amazon, and Google Drive.

## 1.INTRODUCTION

Cloud computing environment gives huge blessings over the local computing surroundings
such as financial value, administrative and management overhead, adaptability, seamless office get right of entry to, less reminiscence utilization, and so forth. Cloud computing gives a platform to customers to utilize various property provided on their request. Cloud computing offers adaptability by way of giving backup facility like Dropbox, Amazon, and Google Drive. Cloud computing also enables clients to cut down their fees by way of supplying surroundings for testing packages without constructing up a bodily domain. It also
offers administrative centers, for example, Software as a Service (SaaS), Platform as a Service
(PaaS), and Infrastructure as a Service (IaaS) [1], [2]. SaaS offers provider to clients, for instance, the virtual work region, webmail, and program interface. PaaS presents a degree for the use of programming language,administrations, libraries, and various apparatuses. IaaS gives online administrations to clients, for example, servers, load balancers, and other computing belongings. Due to those reasons nowadays corporations, corporation and person customers are transferring their information to the cloud. Various fashions of cloud which include private, public, hybrid and community cloud are defined [3] to offer various offerings together with infrastructure, software, and others. The safety of information with overwhelming length inside the cloud is a noteworthy difficulty. Various techniques have been proposed not best to verify facts but also to save you unauthorized get entry to. An over view of cloud computing and related applications.

Data security is a crucial problem even as moving records over the machine having numerous solution proposed within the literature. Be that as it is able to, cryptography is one of the essential methods used to encipher the records utilising either symmetric key or uneven key. The uneven secret's taken into consideration notably relaxed as encryption and decryption use special keys. The key era technique of asymmetric key consumes a large amount of energy and space [4]. Existing proposals have each positives and negatives, for example, Advanced Encryption Standard (AES) is a excessive-protection approach used for encryption [5]. Also, Shamir Secret Sharing Scheme is used for encryption [6]. In [7] touchy records is encrypted with the aid of taking XOR with a random wide variety,break up and allotted over two clouds

## 2. OBJECTIVES

The predominant objective of this undertaking a multi-valued common sense called fuzzy good judgment is used, which has values of truth and variables ranging. It is used where the meanings of fact vary from clearly proper to entirely false. The fuzzy semantic search primarily based on common sense will increase the stop user's search revel in by means of finding and retrieving the equal matching records supplied by way of the user for the corresponding search data. A proficient and relaxed records garage method has been proposed that distributes sensitive users' statistics onto distinct cloud servers to keep away from harm and vulnerability. A mathematical version has been developed and presented
along with encryption and decryption algorithms to encrypt and decrypt touchy as well as everyday

## 3. SCOPE

The safety of statistics with overwhelming length within the cloud is a noteworthy difficulty. Various strategies have been proposed now not most effective to verify statistics however also to prevent unauthorized access. Cloud computing surroundings gives massive advantages over the neighborhood computing surroundings consisting of financial value, administrative and control overhead, adaptability, seamless workplace get right of entry to, less reminiscence utilization, and so forth. Cloud computing presents a platform to customers to utilize numerous property supplied on their request. The proposed PSDS algorithm is primarily based on symmetric key encryption to make certain the confidentiality of the statistics despite the fact that the records is uploaded in elements on distinctive clouds. The proposed approach uploads touchy statistics on multi-cloud so one can protect it from unauthorized get admission to as well as in case of any undesirable situation, all data must not be at a single location

## 5. SYSTEM ANALYSIS

### 5.1 EXISTING SYSTEM

Cloud computing environment gives huge advantages over the local computing environment
consisting of financial value, administrative and control overhead, adaptability, seamless workplace get admission to,less reminiscence usage, and so forth. Cloud computing gives a platform to users to make use of diverse belongings furnished on their request. Therefore, uploading information on a unmarried cloud might also growth the hazard of damage
to the exclusive records. Existing literature observe uncovered multiple cryptography techniques along with SAEDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to secure records garage over multi-cloud. However, current techniques are liable to severa assaults. This article emphasis on facts security troubles over multi cloud and proposes a Proficient Security over Distributed Storage (PSDS) technique. PSDS divides the statistics is into categories; everyday and sensitive,furthermore the touchy records is similarly divided into two parts.

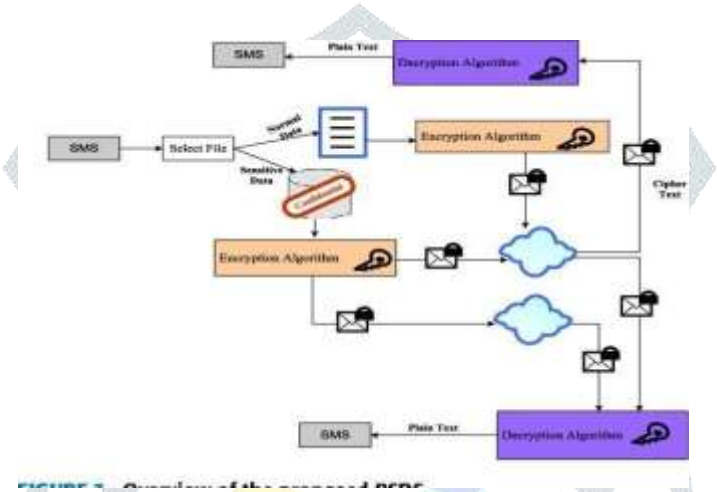
### 5.2 PROPOSED SYSTEM

The standard contributions of this newsletter are: A talented and relaxed statistics storage technique has been proposed that distributes touchy users' records onto distinct cloud servers to a v o i d harm and vulnerability. A mathematical model has been evolved and presented along with encryption and decryption algorithms to encrypt and decrypt touchy in addition to regular records. The proposed approach has been analyzed for protection in opposition to various regarded attack to assess its security. The proposed technique has additionally been analyzed for computation and conversation overhead in case of each touchy as well as everyday statistics to investigate its complexity. A comparative analysis of the proposed method has been presented with AES, STRRNS, RFDA, and SA-DES in phrases of computation time both for sensitive records as well as the overall encryption/decryption time.

6.SYSTEM DESIGN

6.1 ARCHITECTURE DIAGRAM

The machine structure of the proposed approach for record distribution over multi-cloud. Themachine structure includes consumer and cloud garage. A facts proprietor is someone who owns statistics files and a data owner have to Login to add or download a report over the network. After a successful Login, arecords owner may also determine the record kind. Cloud storage is a database that offers a garage location to the customers to save their document(s). Different cloud vendors have exceptional guidelines. An software interface (API) is furnished by cloud service vendors e n a b l i n g users to interact with its offerings. The security of statistics with overwhelming size inside the cloud is a noteworthy problem. Various techniques were proposed not only to verify statistics however also to save you unauthorized get entry to. An over view of cloud computing and associated applications. Data safety is a crucial challenge even as transferring statistics over the machine having various solution proposed within the literature. Be that as it may, cryptography is one of the important techniques used to encipher the facts utilizing both symmetric key or asymmetric key. The uneven secret's taken into consideration surprisingly secure as encryption and decryption use special keys. The key era manner of uneven key consumes a massive amount of power and space.




This article proposes a symmetric key based cryptographic technique named Proficient Security over Distributed Storage (PSDS) to relaxed patron's information over the cloud. The client chooses whether the facts is personal (touchy) or normal (regular) statistics. The private statistics is cut up into two sections, part1 and part2 as seems. After splitting records, encryption steps of PSDS are applied to each elements. Both encrypted parts are uploaded on to 2 separate clouds, cloud 1 and cloud 2 for you to prevent loss or publicity of facts. In the decryption section, touchy information from both clouds is downloaded after which merged each parts. After merging practice the decryption method of PSDS to convert cipher textual content into plain textual content.In the decryption technique of ordinary information, the facts is downloaded from a single cloud after which decryption
is applied to transform cipher textual content to unique text.

6.2 ALGORITHM

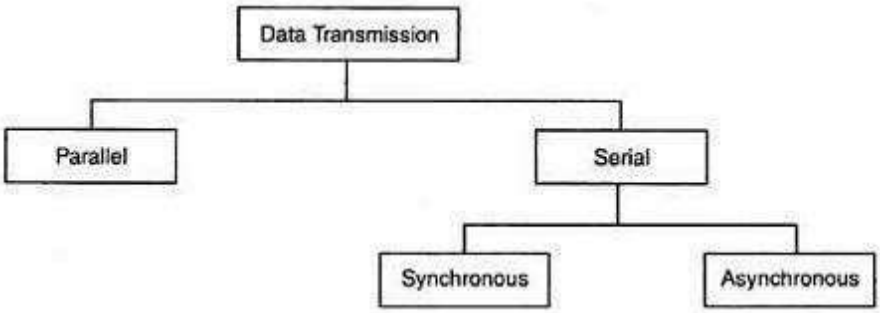
The operating of the proposed PSDS method may be divided into specific components together with; Key Generation – to generate keys for symmetric encryption to make sure the confidentiality of the facts to be saved on the cloud, a splitting set of rules to divide the sensitive statistics into parts, and encryption and decryption algorithms to encrypt records whilst uploading and decrypt it lower back the proprietor wants to get entry to the facts. It can be used as a parameter to gauge computation performance of a selected encryption algorithm. Similarly, to check the overall performance of the proposed PSDS approach, its encryption time each in case of normal as well as sensitive data has been computed. Figure 9 suggests encryption time in milliseconds (MS) of PSDS in case of everyday information. The enter records is taken into consideration byte through byte.

7. SYSTEM IMPLEMENTATION

7.1 LIST OF MODULES

7.1.1 DATA TRANSMISSION

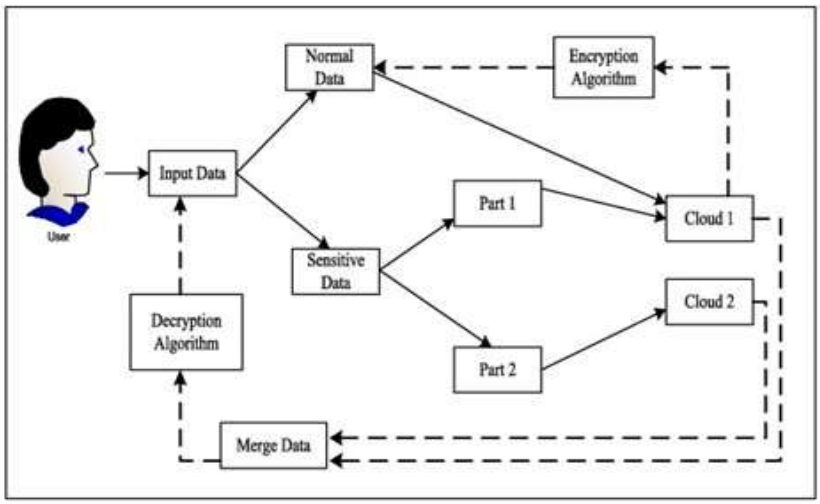
The PSDS is examined towards multiple attacks and it has been concluded that it is proof against related key attack, pollution assault, chosen cipher textual content attack, and recognized plain text attack. Furthermore, PSDS has less computational time as compared to the STTN and RFD encryption technique.




Cloud computing presents a platform to users to utilize numerous property furnished on their request. Cloud computing provides adaptability via giving backup facility like Dropbox, Amazon, and Google Drive. Cloud c o m p u t i n g additionally helps clients to cut down their fees via supplying surroundings for trying out applications without constructing up a bodily area

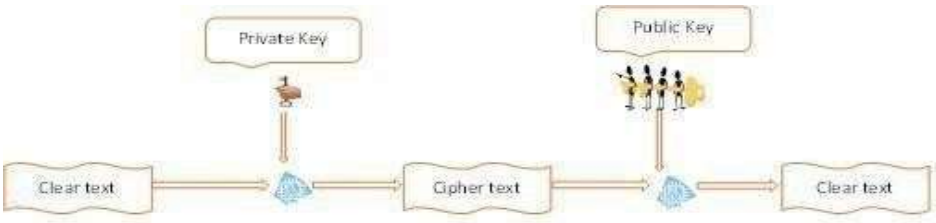
7.1.2 SECURITY

The security of information with overwhelming length inside the cloud is a noteworthy issue. Various techniques have been proposed no longer simplest to confirm information however also to save you unauthorized get right of entry to. An over view of cloud computing and related packages is given. Data security is a important difficulty even as transferring information over the gadget having diverse answer proposed inside the literature. Be that because it can also, cryptography is one of the most important techniques used to encipher the statistics making use of either symmetric key




### 7.1.3. CRYPTOGRAPHIC SOLUTION

PSDS is an adaptable method as it's far designed to obtain high protection by means of splitting touchy facts on a multi-cloud mechanism. The proposed technique resists in opposition to special attacks such as Chosen Cipher text attack, related key Attack, and pollutants assault. It also protects facts towards illegal access via the cloud service vendors.

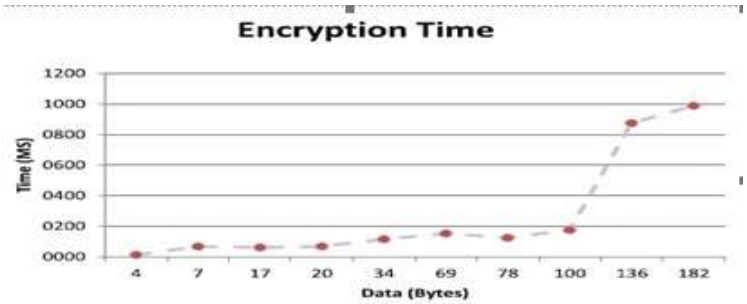



It is used in which the meanings of fact range from certainly true to completely false. The fuzzy semantic seek based on common sense will increase the end consumer's search experience via locating and retrieving the

equal matching records furnished by using the person for the corresponding seek information. In addition, the model makes use of semitone similarities to discover the closest related matches, in situations where the exact matches aren't usable

8. RESULTS AND DISCUSSION

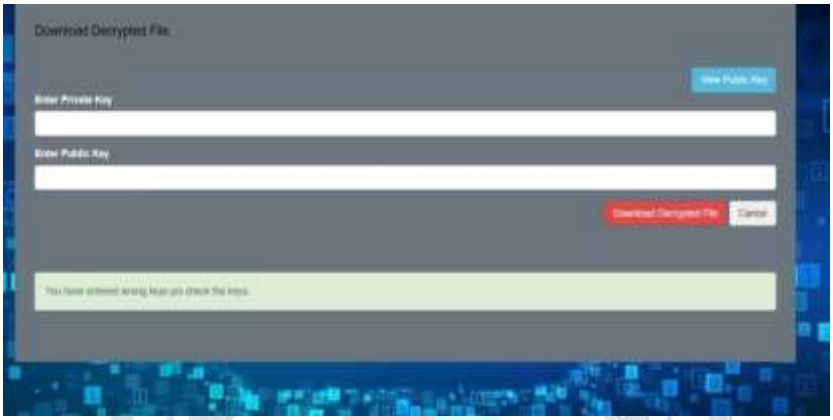
The computational time is an important performance parameter for an encryption approach that indicates how in many instances a certain operation is completed and what's the entire range of operations accomplished at some point of one transactions of a protocol. Computational time is the whole amount of time taken with the aid of an set of rules to finish a specific quantity of computation. The time taken with the aid of key technology technique, Encryption time and decryption time for one-of-a-kind lengths of information. Computational time. The general computational time for 15 bytes is 0089 Ms. It may be seen from the desk that for 21 bytes, the computational time is 0120 MS while the total computational time for 5 bytes is 0050 Ms.

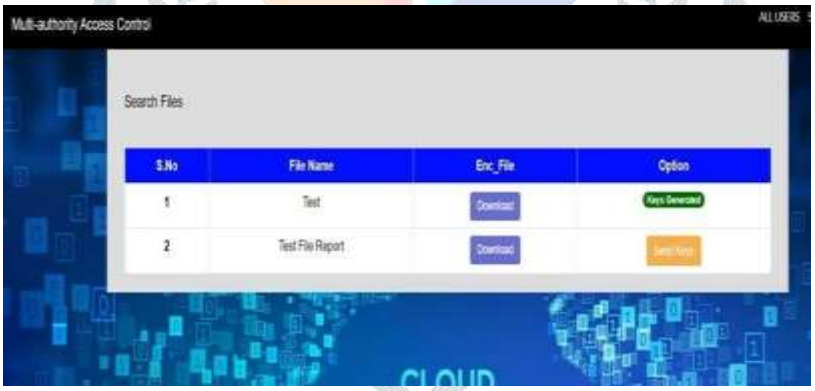



This report consists of analyses and discussions of big problems relating to supervised and unsupervised system getting to know strategies, outlining the blessings and drawbacks of every algorithm, and addressing the scientific findings analysis. Data Veracity for Cloud Storage via Dual Protection (DVCSDP) offers double protection proposed by using Kannan. In the initial step, the file is a part into diverse lumps and dispersed over various servers [43]. Suwansrikham Proposed Asymmetric Secure Storage Scheme (ASSS) [44]. In ASSS statistics proprietor parts the record and accepted the purchaser by way of generating the token which incorporates the username, mystery word, and location. As generation is increasing very hastily, the quantity of facts raises terrifically. Cloud computing will become common among human beings, as human beings can without problems keep their massive quantity of records so one can store memory consumption. The most important issue in storing facts on clouds is records safety. There is a want to switch information into cipher textual content. Multiple procedures are used to comfortable facts over the cloud. Computational time is focused on statistics security approaches. A complex set of rules is not suitable for facts safety because of their growing computational time. The much less complex algorithm has protection problems. In this paper, we advise PSDS so one can remedy the difficulty. In this paper, we propose PSDS in order to remedy the issue. We divide the facts in ordinary and touchy element. Normal records is encrypted and uploaded over a single cloud even as touchy information is split into two components, then encryption steps are implemented on those halves and uploaded on separate clouds. At the time of downloading, those separate halves are merged and the decryption algorithm is carried out with the intention to obtain undeniable textual content. The proposed approach is comfy in opposition to chosen cipher text, known the obvious textual content, related-key assault, pollutants attack, and main-in middle attack.

## 1. SCREEN SHOTS


CLOUD
COMPUTING


Download Decrypted File


Multi-authority Access Control
ALL USERS
Search Files
S.No
File Name
Enc_File
Option
1
Test
Download
Keys Generated
2
Test File Report
Download


Download Decrypted File


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.