2018 International Conference On Advances in Communication and Computing Technology (ICACCT)
Amrutvahini College of Engineering, Sangamner, Ahmednagar, India. Feb 8-9, 2018

Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud

Prachi More
Department of Computer Engineering Indira College of Engineering and Management
Pune, India
Prachimore811@gmail.com

Shubham Chandugade
Department of Computer Engineering Indira College of Engineering and Management
Pune, India
shubhamcg1234@gmail.com

Shaikh Mohammad Shafi Rafiq
Department of Computer Engineering Indira College of Engineering and Management
Pune, India
arman.shaikh751@gmail.com

Prof. Priya Pise
Department of Computer Engineering Indira College of Engineering and Management
Pune, India
priya.pise@gmail.com

***Abstract*— Due to current advancements in cloud computing also the tremendous usage in computing systems, correspondence arrange elevated numerous clients to exchange documents and touchy data through the system, this delicate information requires uncommon arrangement. This work shows a security framework that can give protection and uprightness to trading delicate data through the cloud or the correspondence systems, in view of the utilization of the combination of Attribute-Based Encryption and Byte Rotation Encryption Algorithm. The essence of the work is to build up a straightforward platform that can get protection, integrity, and performance for the data exchange from peer to peer. The proposed framework utilizes symmetric cryptography framework. Data exchange must give end-to-end visibility, security, and consistency.**

Keywords— Cloud Computing, Data Privacy, Authentication, Encryption, Data Security, Data Sharing.

I. INTRODUCTION

As a great deal of private data is being transferred without stopping for even a minute to/from the organizations, there are conceivable outcomes that the data might be lost accidentally or stolen deliberately. This isn't dependable as it could be a genuine risk to the associations. The undertaking is an application to ensure that the information being exchanged over the cloud is secured and private. It is critical that this information being exchanged does not fall into wrong hands to maintain a strategic distance from any money related or enlightening misfortunes that can be destructive to the association. Besides, the capacity of the information and its exchange are gotten to by the approved people just henceforth giving a safe approach to oversee and exchange.

As Cloud Computing becomes popular, more delicate data are being incorporated into the cloud, for example, Messages, financial records, government archives, and so on. By putting away their information into the cloud, the information proprietors can be diminished from the weight of information stockpiling and upkeep in order to appreciate the on-request top-notch information stockpiling administration. Be that as it may, the way that information proprietors and cloud server are not in the same trusted space may put the outsourced information in danger, as the cloud server may never again be completely trusted. It takes after that delicate information, for the most part, ought to be encoded before outsourcing for information protection and fighting spontaneous gets to.

II. RELATEDWORK

Data sharing is winding up progressively essential for some clients and here and there a pivotal necessity, particularly for organizations and associations expecting to pick up benefit. Truly, many individuals saw the PC as "generic monsters" who undermined to slice employments of many individuals through computerization. In any case, as of late, it has been invited by a colossal number of individuals as it has moved toward becoming fundamentally social. It is in this manner not amazing that an ever-increasing number of individuals are requesting information sharing capacity on their telephones, PCs and even as of late Smart TVs. Individuals love to impart data to each other. Regardless of whether it is with companions, family, partners or the world, many individuals advantage extraordinarily through sharing information.

To reduce the computational overhead in mobile computing new Lightweight Data Sharing Scheme (LDSS) is introduced [1]. It receives CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, it changes the structure of access control tree to make it reasonable for versatile cloud situations. LDSS moves a vast segment of

the computational serious access control tree change in CP-ABE from cell phones to outer intermediary servers. Moreover, to reduce the client revocation cost, it acquaints property depiction fields with executing apathetic disavowal, which is a prickly issue in program-based CP-ABE frameworks. The trial comes about demonstrate that LDSS can successfully reduce the overhead on the cell phone side when clients are sharing information in portable cloud situations.

Data security is significant deterrent in various zones like military, bank application, educational organization. Document is forward starting with one area then onto the next area in the organize. Numerous programmers are illegally get to the data. To give answer for this issue many creators has presented diverse calculations and strategies the distinctive calculations like DES, triple DES and AES accomplish greater security however it sets aside more opportunity for encryption and decoding records. A new algorithm is introduced named as Byte Rotation Algorithm [4]. This algorithm gives greater security and takes littlest measure of time for record encryption and decoding. This encryption can apply on various sorts of records like content, picture, sound, video records. In the Byte Rotation Encryption Algorithm include two procedures. One is irregular key generation procedure is utilized, second is parallel encryption and decoding is process utilizing multithreading procedure. Key size of irregular key era strategy is 128 bits. 128bit arbitrary key generation is troublesome for split to assailant.

Attribute based encryption(ABE) is an effective technique that endeavors credits and access approaches to accomplish fine grained get to control in distributed computing. Additionally, extended ABE plans with various authorities (multi-authority ABE) are more reasonable for handy applications than fundamental single expert ABE plans. Existing multi-authority ABE plots either can't safeguard get to arrangements' protection or sustain costly computational cost of encryption and decoding stages. To handle the above difficulties, Jiaye Shao, Yanqin Zhu, QijinJi *proposed* an algorithm [3] on the web/disconnected and outsourced multi-authority ABE conspire with strategy security. Algorithm is developed is to reduce the online calculation overhead for proprietors by part the encryption calculation to the online encryption and disconnected encryption. Amid the decoding stage, clients outsource huge decoding operations to the intermediary server through the method of change key Due to this algorithm [3] most costly encryption operations have been executed in the disconnected stage and the information proprietor simply requires a steady number of online exponentiation operations. With the landing of multi-center CPUs, to accelerate execution of frameworks utilizing parallelism is prompting new approaches. Prior techniques to actualize parallelism in applications were constrained to either utilization of excess equipment assets or direction level parallelism (ILP). This requested the need of part the undertaking or process in too little sections that can keep running in parallel in the errand's unique circumstance, and strings have been presented. Multi-threading is prevalent approach to enhance application execution speeds through parallelism. As each string has it's possess autonomous asset for assignment execution, various procedures can be executed parallel by expanding number of strings. Parallelism is the running of strings in the meantime on centers of a similar CPU. Multi-threading is famous approach to enhance application execution speeds through parallelism [5]. Initially it is presenting the diverse security and protection safeguarding strategies for distributed computing and enormous information stages with their restrictions, half system for secure delicate information sharing and protection saving open inspecting for shared information over huge information frameworks including functionalities such as protection saving, open reviewing, information security, stock piling, information access, erasure or secure information obliteration utilizing cloud administrations[7].

To beat a security challenge, an effective information encryption calculation for encoding touchy information before sending it to cloud is being proposed and executed. It tends to piece-level information encryption by utilizing a symmetric key. In this examination work, we researched the issue of sharing delicate information on cloud stage utilizing DES and BASE-64 calculations in the coordinated effort. The exploratory examination for piece-level information encryption has been performed on assortment sorts of the document which are outsourced from archives. Examination demonstrates a proposed communitarian strategy is very proficient regarding time and security levels [6]. To make Attribute-based encryption (ABE) more appropriate for getting to control to information put away in the cloud. Principal result is an expansion of the decentralized CP-ABE plot of Lewko and Waters [LW11] with personality-based client disavowal [8].

III. PROPOSEDSYSTEM

A. Hybrid ABE and BREA

To address privacy issue in existing system is proposed a crypto-system for secure sharing of data over the cloud, which uses combination Attribute Based Encryption and Byte Rotation Encryption Algorithm in combination with each other. To provide extra security and privacy for data sharing and collaboration in the cloud.

Attribute-Based Encryption algorithm will identify the attributes of the data to be uploaded. These attributes will help the BREA to understand the type of data is to be encrypted after identifying the data type of the file BREA will perform either single, multi or hybrid phase encryption.

After Encryption of the data a random key will generated using ABE which will the user to decode the encrypted file. With the combination of 2 ABE and BREA we are proposing a crypto-system which can run on all limited resources devices. It can take data from the user and provide off-line-online service.

B. Advantages

1) Here data can be transferred from one user to another securely over the cloud.
2) The system cost will be decreased.
3) It will work on all limited resource devices.

C. Proposed System Encryption and Decryption Algorithm

In our proposed system data is encrypted before uploading to the cloud. Combination of Attribute Based Encryption and Byte Rotation Algorithm are used for the encryption of the data. ABE will help to identify the attributes of the data and BREA will perform matrix operations on the block of the data to been crypted.

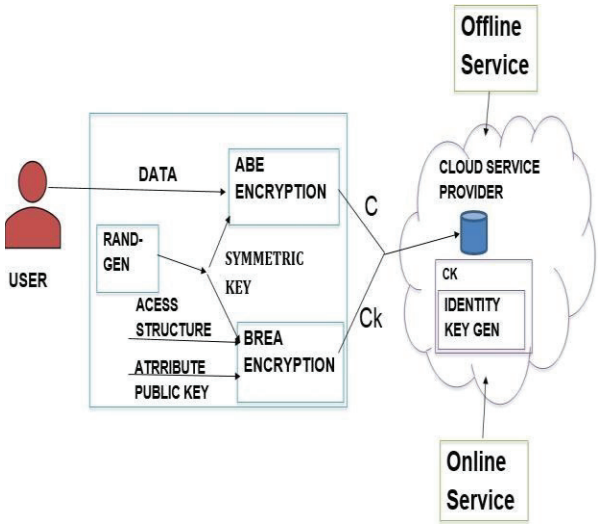

Fig 1: Encryption

After performing encryption operation, a random key is generated alongside the encrypted data. Data will be send in encrypted format to respective user. To decrypt this data receiver has to enter the One Time Password (OTP) which will be matched with key generated using ABE algorithm.

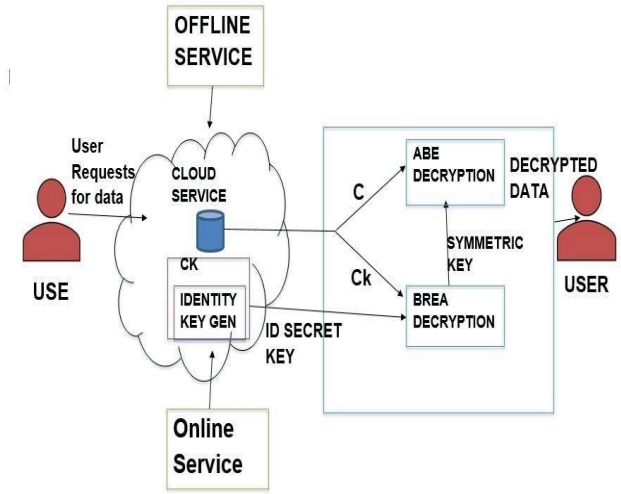

Fig 2: Decryption

D. Proposed System Algorithm

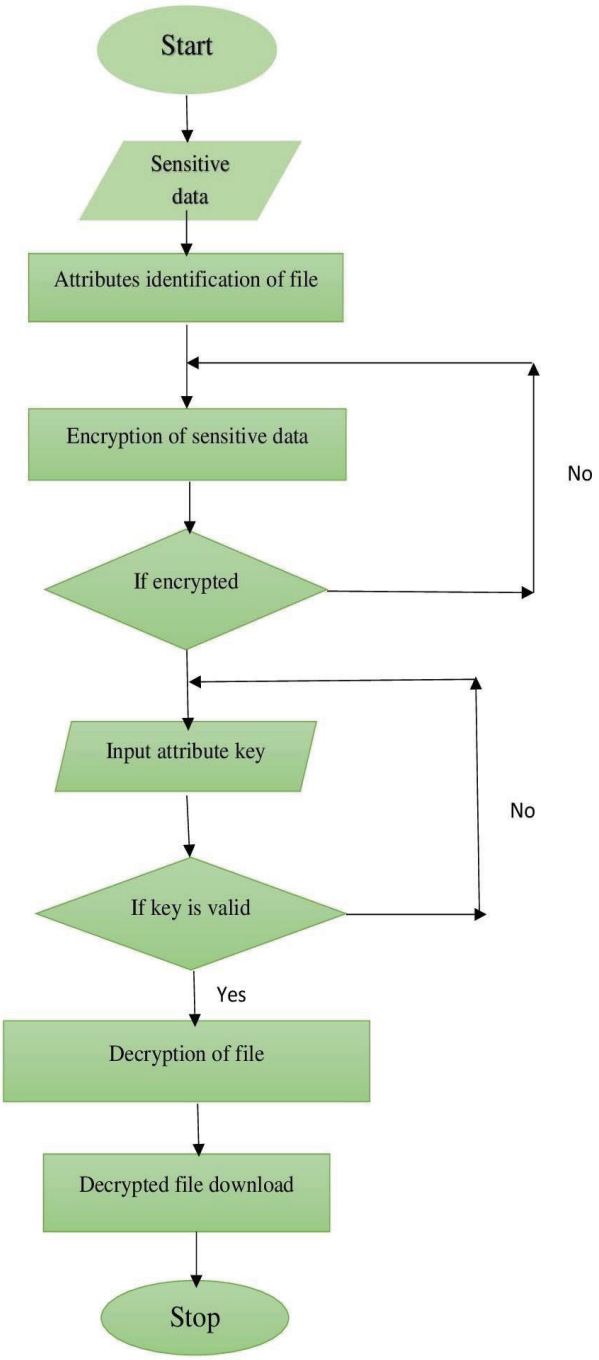

Fig 3: FlowChart

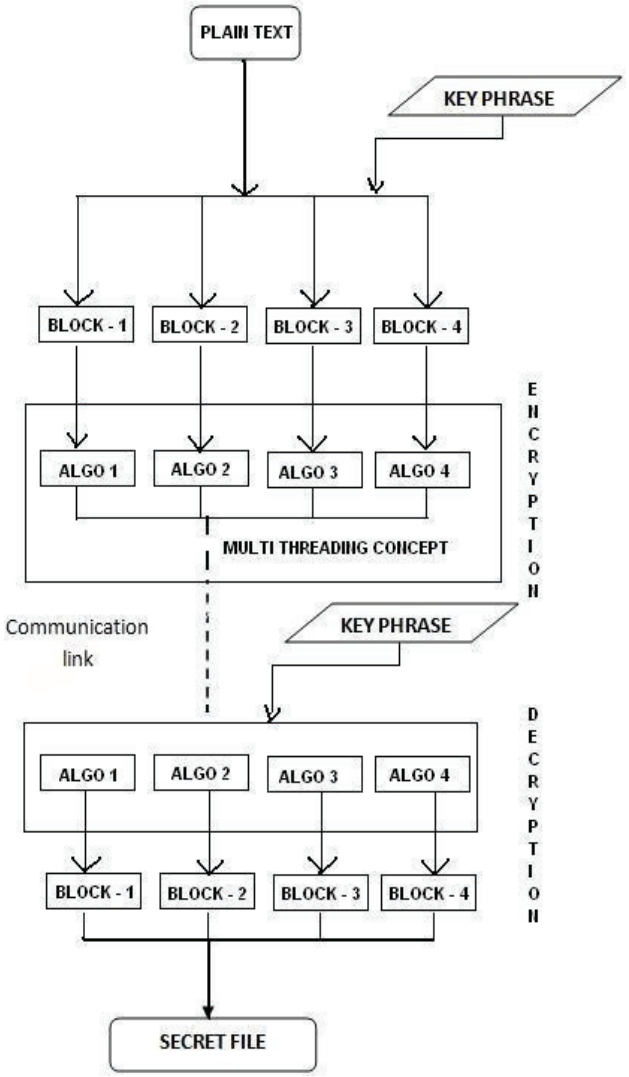

Fig 4: Data Flow

IV. CONCLUSION

In this paper, the issue of sharing the data in cloud computing securely is resolved. The different methods of secure data sharing and privacy preserving is discussed in related work. Authentication is used to guarantee data privacy and data integrity. Based on the literature study, we have introduced hybrid algorithm. Data privacy can be maintained by combination of ABE and BRE algorithm. This indicates that the proposed system can be used to enhance privacy preservation in cloud services. For future work we will like to make our system heterogeneous so that it will be able to work on any machine or platform.

REFERENCES

[1] A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing Ruixuan Li, Member, IEEE, ChenglinShen, HengHe, ZhiyongXu, and Cheng-ZhongXu, Member,IEEE

[2] Privacy-Preserving Online/Offline and Outsourced Multi- Authority Attribute-BasedEncryptionJiayeShao†,YanqinZhu†∗ ,QijinJi† †School of Computer Science andTechnology, Soochow University

[3] Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security PunamMaitriDattatrayS.WagholeVivek S. Deshpande, IEEE Senior Member 2015 International Conference on PervasiveComputing(ICPC)

[4] Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-like Block Ciphers SikharPatranabis, AbhishekChakraborty, DebdeepMukhopadhyay, and P.P. Chakrabarti Department of Computer Science and Engineering IIT Kharagpur, India IEEE2017

[5] Analysis of multi-threading time metric on single and multi-core CPUs with Matrix multiplication Dhruva R. Rinku, Dr. M Asha Rani 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics(AEEICB17)

[6] PriyaDudhalePise,Dr. Nilesh J Uke,"Efficient Security Protocol for Sensitive Data Sharing on Cloud Platforms" in2017IEEE.

[7] PriyaDudhalePise,Dr. Nilesh J Uke,"EfycientSecurity Framework for Sensitive Data Sharing and Privacy Preserving on Big-Data and Cloud Platforms." in 2017 IEEE.

[8] Mate Horvath," Attribute-Based Encryption Optimized for Cloud Computing.."

[9] Yang Yang, Attribute-based data retrieval with semantic keyword search fore-healthcloud.