Secure Data Extrication for Demoralized Disruption Tolerant Network

Priyanka C.Atre
Department of Computer, Sandip Institute Of Engineering(Nasik), A/P.Sinnar
Rachana L.Pawar
Department of Computer, Sandip Institute Of Engineering(Nasik), Nasik Road,Nasik
Pranali A.Shinde
Department of Computer, Sandip Institute Of Engineering(Nasik), Soygaon,Malegaon

ABSTRACT
Steganography is one of the important concept which is used for Encryption and Decryption purpose. There are some issues of cloud storage like confidentiality, data integrity and data availability. So the "cloud" is a collection of distributed super computers spread across the world, authentication and authorization for information access is more than a necessity. In this paper ,we try to overcome these security threats. In our proposed system the encryption of the User's Sound is to be uploaded on the cloud. The integrity and confidential information which is uploaded by the user is not only encrypting it as well as providing access to the data only for authenticated person.

Keywords
Steganography, Disruption tolerant network (DTN), Cipher text-policy attribute-based encryption (CP-ABE), information recovery, secure data retrieval.

1. INTRODUCTION
Networking is the word related to computers and their connectivity. It is very useful in the world of computers and their need in different connections. The concept of networking is provide the link between two or more computers and their devices, with the main purpose of sharing the information stored in the computers, with each other. There are number of characteristics of networking like availability, reliability, security, speed, scalability, topology etc. There are number of networks in which lot of secret information is exchange. In some of the network, the Authorized person for the group act as a key authority. In before that every user is need to register in the portal and specific password and id is give to each user .By using Id and password ,they can transmit the information for the specific user and they can have specific communication device and from that device they can transfer the Information, in which for them for the particula region,particular key authority are there and they can get key from authorized person.[1]. For this purpose DTN (disruption-tolerant -network) Technology is useful. The encryption policy is used for security purpose in which CPABE(Cipher text-policy attribute-based encryption)technology is used. The CP-ABE(Cipher text policy attribute-based encryption)technology is one of the different and important technology which is based on attribute base. [9]The information which is needed that are taken in encrypted form by getting the key from the authority .There is individual authority for group member and for key update same algorithm is used. .If the old existing user remove account from that group then that will be inform to the key authority and account is expired. Unauthorized person not able to view.The ABE (Attribute-Based Encryption) is one of the encryption technique that is different from other Encryption techique and make it secure for the existing members of group [3].If any member of group is remove, then it's unique Id i.e.IMEI (International Mobile Equipment Identity) Number is also remove and if the new member is joined, the same IMEI (International Mobile Equipment Identity) Number is not given, it is different from old IMEI(International Mobile Equipment Identity) Number .All material on each page should fit within a rectangle of 18 x 23.5 cm (7" x 9.25"), centered on the page, beginning 2.54 cm (1") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (.75"). The text should be in two 8.45 cm (3.33") columns with a .83 cm (.33") gutter.

2. LITERATURE SURVEY
Junbeom Hur [1], etc.al in there paper " Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" proposed that ,the key escrow problem is resolved by an escrow-free key issuing protocol. Immediate attribute revocation increases backward/forward secrecy of confidential data by reducing the windows of vulnerability

Arshiya Tabassum[2], etc.al in paper " Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" in these paper, encryptors can define a fine-grained access policy using any access structure under attributes issued from any chosen set of authorities .it also gives an overview and working principle of the technology including its advantages, Challanges.

S.Revathi [3], etc.al " Advanced Data Access Scheme in Disruption Tolerant Network " presents CP-ABE is used to generate a private key of user based on their attribute keys. Every time when a user enters or removes from certain group then immediate key revocation is done. Updating attribute is not so efficient for every changes and it produces high computation complexity and communication cost. this drawback is overcome in this paper.

Hoovesha M. J. (**[4],**etc.al in there paper " Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", propose that ,to provide computerized cloud storage as well as easy retrival of crime and criminal recoreds.

S. Chitra [5] etc .al propes in there paper "Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm " that using Cipher text Policy Attribute Based Encryption (CP-ABE) for secures data retrieval in disruption tolerant military network. Key escrow problem is resolved in the military network as well as they attempt to enhance the existing secure date retrieval model of decentralized disruption tolerant military networks with providing Source Anonymity

1K. Kalaiselvi [6], etc.al in there paper "Cipher Text-Policy Attribute based Encryption for Secure Data Retrieval in Disruption-Tolerant Military Networks (DTN) " proprosed that Cipher text-Policy Attribute Based Encryption (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the descriptor needs to possess in order to decrypt the cipher text.

M. A. Lokhandwala [7], etc.al in there paper " Key Escrow Removal Using Random Oracle in CP-ABE for Security in Military Networks" represents that, Confidential Data Security Methodology has been modified by using random key authority generation replacing two-party computation protocol to remove the disadvantage KEY ESCROW, with recent adoption and spreading of data sharing.

Korra Bichya [8], etc.al in there paper " Secure Information Recovery for Decentralized Interruption Tolerant Defense Data Network "they propose a property based secure information recovery plan utilizing CP-ABE for decentralized DTNs. The proposed plan emphasizes the accompanying accomplishments.

Rasika S. Rangari [9], etc.al propose in there paper " Review Paper on Highly Secure Data Communication Between Two Decentralized Army Stations " that, it is a desirable to provide a differentiated access services that a Data access policies are defined over a user attributes or a roles, which are managed by the key authorities.

S.Suseela [10] etc.al in there paper" Fastened Data Retrieval Algorithm (FDRA) " they describes the an adaptively secure d id entity-based broadcast encryption (IBBE) scheme based on the hard worst-case lattice problems .

3. PROPOSED SYSTEM

3.1 Aim

Here we are focusing on the security of transmit the data from one location to another location .we also reduce the time complexity of existing system.

3.2 Objectives

- How can we send the information secretly to the Destination.
- Using this system ,information can be hidden in carriers as text files and data is transmitted.
- In this proposed system, we create new framework which converts user's voice into text and send it to the Destination.

The Attribute-Based Encryption(ABE) is one of the important approach which is uesful for Safe information extrication using DTNs(Delay Tolerant Network). The encryption techique is used for security purpose in which CP-ABE (Cipher text-policy attribute-based encryption) technology is used. The CP-ABE(Cipher text-policy attribute-based encryption)technology is one of the different and important technology.The information which is needed that are taken in encrypted form by getting the key from the authority .There is Seperate authority for group member and for key update same algorithm is used. The encrypted data is stored into storage node.[3] The system diagram as shown in following figure.

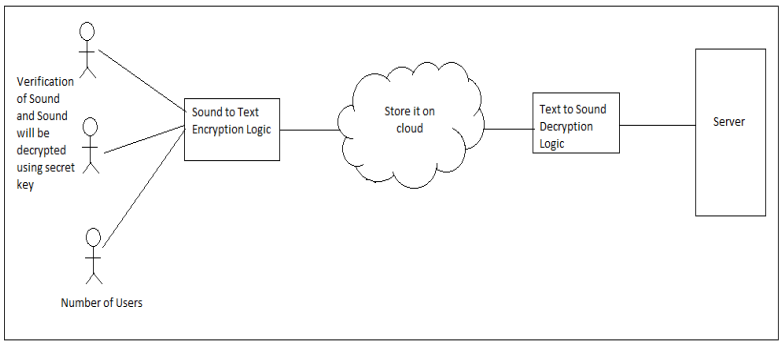

Figure .system Architechure

From storage node, required information can be able to take by group member. There is one of the challenge in which co-ordination of the key authority is important and user who are the holding account in that and in which previous the key escrow

problem is exist and now this problem is overcome, in which all the key authority are not able to view the key of group members and in which particular key authority can see their own group member's key and remaining key authority cannot view.

4. DESIGN AND SPECIFICATION

Let 'S' be a techique which is for safe data retrival.

Such that,
S= {A, M,L,O,}

Where,
1)'A' represents encryption algorithm;
2)'M' represents decryption algorithm;
3)L' represents set of Storage Cloud;
L={l0,...,l n| l}
L={D,W,T,K,M}
Where,

a) 'D' represents Sound data;
D={I0....,I n| d}
b) 'W' represents Key data;
W={w0,....,w n| w}
c) 'T' represents Sound Encryption.
d) 'K' represents Key management.
e) M' reprsents Sound Decryption.
f) 'O' represents set of Output.
Such that,
O={O1,O2,...On| S}
Where,
a) O' represents Retrived Sound.\

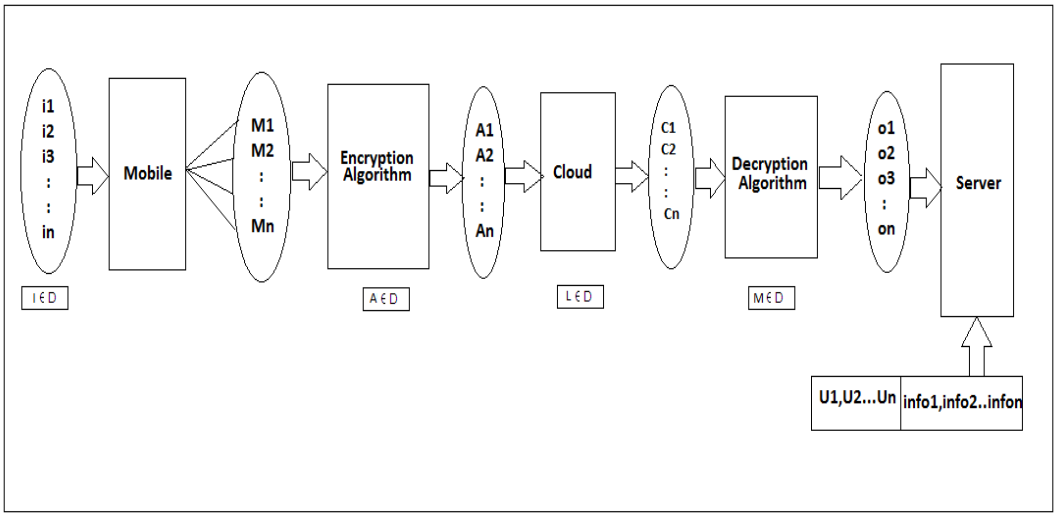

Fig 2:Mathematical Model

5. Conclusion

The developed project achieved the many goals like authentication and providing security on cloud storage node.. we achieved data encryption during the storing of the sound text data files. This ensured that the content to be safe and secure. This concludes us in saying that the goals that were set during the development of the project have been achieved as desired and the project is ready for large scale implementation or for commercialization

6. ACKNOWLEDGMENTS

We are sincerely thankful to all the researchers for the well-defined problematic suggestions. we are thankful to Prof. S. A. Ahirrao for his guidance and useful discussion through different faculties.

3. REFERENCES

[1] "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" by Junbeom Hur and Kyungtae Kang, Member,in IEEE TRANSACTIONS ON NETWORKING VOL:22 NO:1 YEAR 2014

[2] "Secure Data Retrieval For Decentralized Disruption Tolerant Military Network" by Miss. Arshiya Tabassum R.A.Khan, **Miss.Ashwitha Reddy. In International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences (NCDATES- 09th & 10th January 2015)

[3] "Advanced Data Access Scheme in Disruption Tolerant Network" by S .Revathi , A.P.V .Raghavendra in International Journal of Innovative Research in Computer and Communication Engineering.

[4] "SECURE DATA RETRIEVAL FOR DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS"by HOOVESHA M J and SANJAY H M in International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June-2015, pg. 324-333

[5] "Privacy Preserving and Secure Data Retrieval in Sensor Network using Homomorphic Encryption Algorithm" by S.Shanmugasundaram and S.Chitra in International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 12 Issue 3 –JANUARY 2015.

[6] "Cipher Text-Policy Attribute based Encryption for Secure Data Retrieval in Disruption-Tolerant Military Networks (DTN) " by K. Kalaiselvi and B.Kabilarasan in International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 11 Issue 3 –NOVEMBER 2014

[7] "Key Escrow Removal Using Random Oracle in CP-ABE for Security in military network" by Hiral Patel,M.A. Lokhandwala in international Journal of Advanced Research in communication and computer Engineering.

[8] "Secure Information Recovery for Decentralized Interruption Tolerant Defense Data Network "by Korra Bichya in INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 3, SEPTEMBER 2014, PP 119-126

[9] " Review Paper on Highly Secure Data Communication Between Two Decentralized Army Stations "by Rasika S. Rangari , Prof. Anil N. Jaiswal in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume4, Issue 1, April 2015

[10] " Fastened Data Retrieval Algorithm (FDRA)" by S.Suseela#1, B.Purushotham in International Journal of Computer Trends and Technology (IJCTT) – volume 23 Number 3 – May 2015