IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

A Survey on Secure Information Exchange via Military Networks Using Different Encryption Technique

Mr.Ankush Pawar, Dr A.A.Gurjar

PG Student, Dept. of I.T, Sipna College of Engineering Technology and Research Amravati, India

Assistant Professor, Dept. of I.T, Sipna College of Engineering Technology and Research Amravati, India

ABSTRACT: DTN technologies are fast becoming famous an functional solutions in military applications that permit or enable wireless devices in the network to communicate with each other and access the confidential data infallible or in a trustworthy manner by utilizing the storage nodes.This paper considers an attribute-based secure data retrieval scheme using CP-ABE for ITNs where multiple key authorities manage their attributes independently. Immediate attribute repeal enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing protocol that utilizes the characteristic of the decentralized ITN architecture proposed a decentralized approach; their technique does not authenticate users. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the Interruption-tolerant military network. key escrow, and coordination of traits issued from various powers. This work introduce a secure information recovery plan utilizing CP-ABE for decentralized DTNs where number of key powers deal with their properties autonomously. This shows how to apply the proposed system to safely and effectively deal with the private information appropriated in the interruption tolerant military system**.**

KEYWORDS: Certificate authority (CA), attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

I. INTRODUCTION

Network provides a sharing of data among different users with the help of wireless devices. For this, a network must provide a secure communication among the network for data transfer to the entire user in the network. With the wireless network, transfer of data where done with the help of the intermediate node, here data may be lose because of unauthorized user in the network may hack the data. Disruption-tolerant network (DTN) is a technology which allows the node to communicate with each other in secure manner [1]. It is one of the successful solutions for transferring the data in network. Most of the military users use this technology for secure transfer of the data. In the large number of outgrowing commercial environment such as military each and everything based on the another sources to broadcast the data strongly and maintain the
data as well in the regular medium. Usually, when there is no end-to-end communication among a source and destination pair, the data from the source node may want to stay in the intermediate nodes for an extensive amount of time until the connection would be ultimately` established.

. The Attribute Based Encryption (ABE) [11] is a methodology that gives secure information recovery in Disruption Tolerant Networks. This component empowers an entrance control over encoded information utilizing access arrangements and qualities among private keys. The Cipher content Policy Attribute Based Encryption (CP-ABE) [5], which is one of the critical kind of ABE plans, gives a versatile method for encoding information such that the encryptor characterizes property set that the descriptor needs to have so as to unscramble the figure content.

The issue of applying the ABE to DTNs[1] presents a few protection and security challenges. The primary test is the key repudiation issue. A few clients might change their characteristics sooner or later of time, so key repudiation for every property is vital so as to make the frameworks secure. However, this issue is more troublesome in ABE frameworks, since numerous clients shares every quality. Consequently denial of any property or any single client in a quality gathering might influence alternate clients in the gathering.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

The key escrow issue is another test. In CP-ABE [5], the private keys of clients are produced by the key power, by creating their trait keys. This could be a potential risk to the protection or information privacy, if the key power is traded off by a few enemies.

The last test is the coordination of properties. At the point when various powers issue and oversee ascribe keys to clients freely with their own particular expert mysteries, it is hard to characterize fine-grained access approaches over the characteristics issued from various powers.

II. LITERATURE SURVEY

B. D. Huang and M. Verma [4] Planned a theme within the multi authority network surroundings referred to as decentralized Cipher text-policy Attribute-based encryption (CP-ABE). They achieved a combined access policy by encrypting the information multiple times over the attributes issued from multiple authorities.
F. Chase and S. M. Chow [8] Given a distributed key-policy Attribute-based encoding (KP-ABE) scheme that solves the key written agreement drawback in an exceedingly multi authority system. During this theme, participating to get attribute keys mistreatment the key generation protocol in an exceedingly distributed method such they can't collect their information and acquire attribute sets that are happiness to an equivalent user.

J. Bethencourt give construction of a cipher-text-policy attribute-based encoding (CP-ABE). during this system, a user's non-public key are going to be connected with a random variety of attributes verbalized as strings. Conversely, once a celebration encrypts a message in expressed theme, they specify connected access structure over attributes. In this, a user are going to be able to rewrite a cipher-text if and as long as user's attributes pass all the means through the cipher-text's access formation [5]
.

In paper [8] Luan Ibraimi propose a replacement system meant for attribute revocation in CP-ABE called mediate Ciphertext-Policy Attribute-Based encoding (mCP-ABE). during this system the key key's divided into 2 components, 1st share for the intermediary and also the second for the user. To rewrite the data, the user is needed to contact the intermediary to just accept a coding token. The intermediary conducts associate degree attribute revocation list ARL and trashes to issues the coding token for revoked attribute. innocent of the token, the user cannot rewrite the cipher-text, therefore the attribute is totally revoked.

P. Yang and M. Chuah et al [7] analyze several approaches for the distribution of data in the network, and they have been proposed for multicast routing in DTNs presumptuous the accessibility of dissimilar amounts of knowledge a bout network topology, etc. and they have propos context-aware adaptive multicast routing(CAMR) approach to switch different network situation improved performance than the existing approach of multicast rescue schemes for DTNs. Their approach is to address the confronts of opportunistic association connectivity in DTNs.

III. PROPOSED SYSTEM

In this paper, we propose securing secure exchange information via military network there are number of wireless device used in military network but another third party easily access these top secrete information. Disruption-tolerant military networks (DTNs) using ciphertext-policy attribute-based encryption (CP-ABE) and different encryption technique. Like a cipher-text this is the scrambled message produce as output .The proposed scheme The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over private and master keys, and cipher texts (CPABE).Scalability is provided by CP-ABE for data encryption and decryption. ABE enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Encryptions define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.. We show how to apply the proposed scheme in securing and effectively manage the confidential data distribution in the DTN network. The projected theme options the subsequent achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential information by reducing the windows of vulnerability. Second, encryptors will outline a fine-grained access policy exploitation any monotone access structure underneath attributes issued from any chosen set of authorities. Third, the key written agreement downside is resolved by associate escrow-free key provision protocol that exploits the characteristic of the suburbanized DTN design. The 2PC protocol deters the key authorities from getting any master secret info of every different such none of them might generate the full set

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

of user keys alone. Thus, users don't seem to be needed to completely trust the authorities so as to guard their information to be shared. The information confidentiality and privacy will be cryptographically enforced against any curious key authorities or data storage nodes within the projected theme.

Key Authority Create a different key and send to sender side and receiver side sender we can send a secrets information to receiver using a public key and receiver decrypt this information using private key. Every attribute key of a user can be modified independently and instantly. Hence, the security and scalability can be improved in the proposed system.

IV. PROPOSED WORK

I) To propose an attribute based secure data for the transaction of data retrieval using digital signature.
II) Key-Issue Protocol generates and issues the secret key for user.
III) Key-Issue Protocol generates and issues the secret key for user.
IV) Digital Signature is used for Key Authorization.
V) In, the two PC protocol the key authority act as master secret for sharing information.

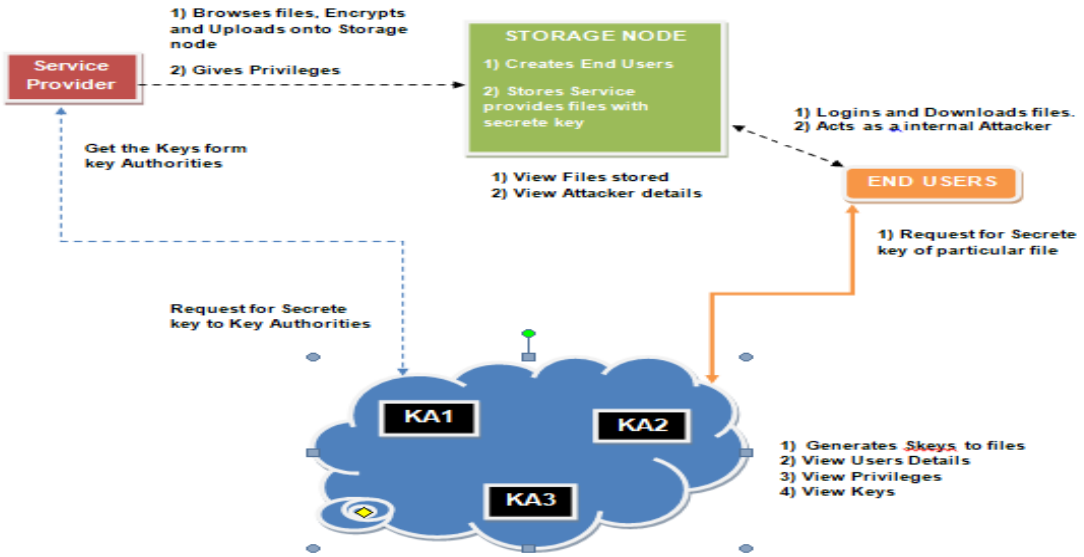

Fig. 1. Architecture Design of DTN

As in figure 1, the entities can explain as follows.

A. Key Authorities

They are the key era focuses that produce open or mystery parameters for CP-ABE. The key powers comprise of focal power and numerous neighborhood powers. There are secure and dependable correspondence channels between a focal power and every neighborhood power. Every neighborhood power oversees diverse traits and issues relating ascribe keys to clients.

B. Storage node

This is an entity that stores information obtains from senders and forward equivalent access to users. Storage node may be mobile or static [5], [6] depend on application in which it is used.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

C. Sender

This is an entity that sends mystery messages or information (e.g., a commander in case of military) and desires to store these messages into the external information storage node for simplicity of data sharing or for consistent delivery to users in the intense networking environments. A sender is dependable for essential (attribute based) access rights and accomplishing it on its own data by encrypting the information under the policy previous to storing it to the storage node.

D. User

This is a node who requests to access the information stored at the storage node (e.g., a soldier in case of military). If a user possesses a set of attributes fulfilling the access policy of the encrypted data distinct by the sender, moreover is not revoked in any attributes, so that then user will can decrypt the Cipher text and get the original data.

V. AES ALGORITHM OVERVIEW

Key Expansion:

The AES (Advanced Encryption Standard) algorithm operates on blocks of data, typically 128 bits in length, and supports key sizes of 128, 192, or 256 bits. Before encryption begins, the key is expanded to create a key schedule containing a set of round keys.

Initial Round:

The input block of plaintext is XORed with the first round key.

Rounds:

AES consists of multiple rounds, with the number of rounds determined by the key size:

For AES-128, there are 10 rounds.

For AES-192, there are 12 rounds.

For AES-256, there are 14 rounds.

Each round involves the following steps:

SubBytes: Each byte of the block is substituted using a substitution box (S-box).

ShiftRows: The rows of the block are shifted cyclically.

MixColumns: Each column of the block is mixed using a matrix multiplication operation.

AddRoundKey: The round key is XORed with the block.

Final Round*:* In the final round, the MixColumns step is omitted.

Output*:* After the final round, the resulting block is the ciphertext.

Example AES Encryption Process:

Let's illustrate the AES encryption process using a simplified example with a 128-bit key:

Plaintext*:* "HELLO WORLD12345" (16 bytes)

Key: "SECRETKEY1234567" (16 bytes)

Key Expansion: The 128-bit key is expanded to create a key schedule with 11 round keys.

Initial Round:The plaintext block is XORed with the first round key.

Rounds*:*Each round consists of SubBytes, ShiftRows, MixColumns, and AddRoundKey operations.

Final Round:The MixColumns step is omitted in the final round.

Output:

The resulting ciphertext block is the encrypted form of the plaintext.

Decryption:

Decryption using AES involves the reverse operations of encryption:

The ciphertext block is XORed with the final round key.

The inverse of each round operation (InvSubBytes, InvShiftRows, InvMixColumns) is applied in reverse order.

The resulting block is the decrypted plaintext.

AES is widely regarded as secure and has been extensively analyzed by cryptographers. Its security relies on the strength of the key, with longer key sizes providing increased resistance to brute-force attacks. AES has been adopted as a standard encryption algorithm by governments and organizations worldwide for securing sensitive information.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

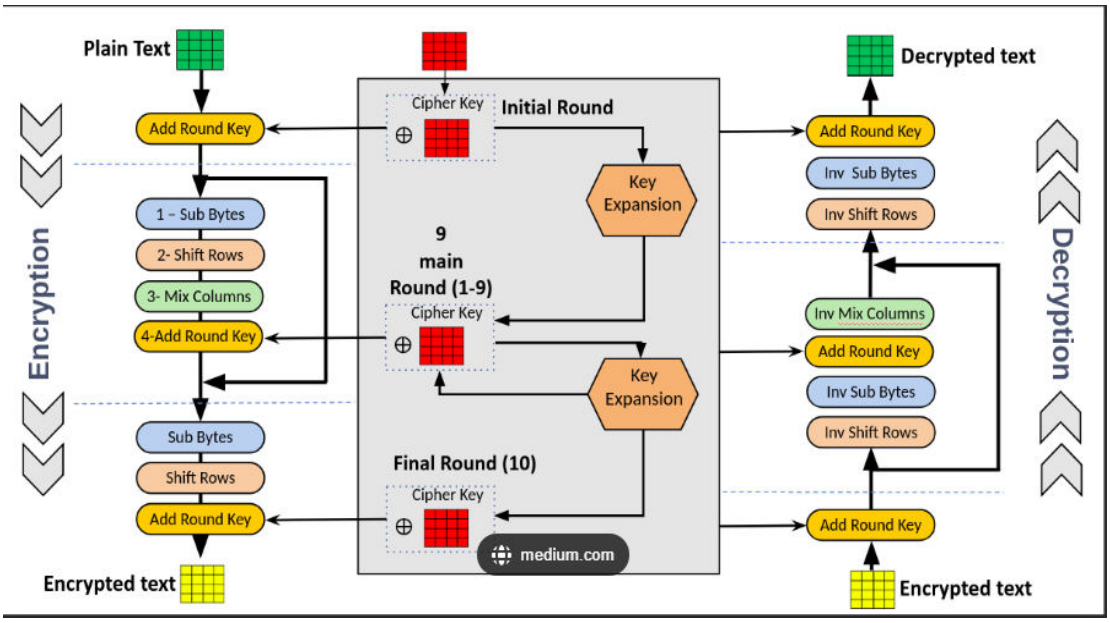

Figure 4.8.1 AES Algorithm Flow Chart

VI. SECURITY REQUIREMENTS

1. Unauthorized users who do not enclose enough credentials fulfilling the access policy should be blocked from collecting the simple user information in the storage node. And illegal access from key authorities node should be in addition prevented.
2. If numerous users get together, they may be capable to decrypt a Cipher text by concatenating their attributes still if every one of the users cannot decrypt the Cipher text by himself. Furthermore believe collusion attack between interested public authorities to get users' keys.

VII. CONCLUSION

Nowadays, DTN technologies are taking successful position for solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. Cryptographic solution is CP-ABE which has access control and secure data retrieval issues

This paper presented a CP-ABE system which we can use in Disruption Tolerant Networks to the access control and prevents data retrieval problems, CP-ABE is an extensible cryptographic solution. This paper focuses a secure and valuable information retrieval technique via CP-ABE for decentralized DTNs where numerous key authorities to handle their attributes separately. The problem of inherent key is solved in such way that the privacy of the stored data is guaranteed even under the antagonistic environment where main core authorities might be negotiated or not completely trusted.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", member IEEE, ACM, Feb 2014.
[2] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.
[3] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
[4] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307116|

[5] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[6] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc. Conf. File Storage Technol.*, 2003, pp. 29–42.
[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.
[9] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.
[10] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.
[11]A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351,2010.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details