International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

High Secured Attribute Encryption Based System for Military Data Retrieval

Snehal Gaikwad[1], Suhas Patil[2]

[1]Department of Computer Engineering, KJCOEMR, Pune, India

[2]Professor, Department of Computer Engineering, KJCOEMR, Pune, India

Abstract: ***Portable hubs in military situations, for example, a combat zone or an antagonistic locale are prone to experience the ill effects of discontinuous system network and visit parcels. Interruption tolerant system (DTN) advancements are getting to be useful arrangements that permit remote devices conveyed by fighters to correspond with one another and access the classified data or summon dependably by abusing outside capacity hubs. The absolute most difficult issues in this situation are the requirement of authority arrangements and the strategies upgrade for secure information recovery. Ciphertext-arrangement characteristic based encryption (CP-ABE) is a promising cryptographic answer for the entrance control issues. The issue of applying CP-ABE in decentralized DTNs presents a few security and protection challenges with respect to the characteristic denial, 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.

1. Introduction

As the systems are growing broadly, correspondence security over the Internet is turning out to be more vital. Cryptography is one of the principle field of examination which is utilized to improve the correspondence security. The different cryptography systems are DES, RSA, and ABE, which are solely used to encode, which is the procedure of changing over plaintext into figure content. After information encryption, the mystery information seems, by all accounts, to be good for nothing bits. Encryption keeps away from unapproved client to unscramble or obliterate it.

The Attribute Based Encryption (ABE) [10] 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 and figure writings. The Cipher content Policy Attribute Based Encryption (CP-ABE) [8], 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 decryptor needs to have so as to unscramble the figure content.

2. Related Work

S. Roy [5] and P. rule [6] introduces knowledge storage nodes in DTNs wherever user info is replicated during this method that just approved mobile nodes be able to access the essential info quickly and expeditiously.

In Paper [5] authors S. Roy and M. Chuah introduced associate degree access management mechanism that is looking on the Ciphertext Policy Attributed-Based secret writing (CP-ABE) paradigm. The system provides a supple fine-grained access control in such method that the encrypted knowledge will be accessed by solely approved users. System provides 2 distinctive features: (i) the incorporation of dynamic attributes whose value could vary over amount, and (ii) the revocation characteristic.

In Paper [6] M. Chuah, P. rule explored that however a Content based info retrieval theme will be deliberate for DTNs. There square measure 3 important style errors, specifically (a) however ought to info be replicated and the way will it's keep at varied nodes, (b) however ought to a question be distributed in gently connected networks, (c) however ought to a question reply be routed back to the querying node.

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 attributes. innocent of the token, the user cannot rewrite the ciphertext, therefore the attribute is totally revoked.

In [9] author N. bird genus introduced attenuation perform, that provides attributes ”dynamic” and permits United States of America to switch each one amongst them severally to stay electronic equipment information measure, resources and time. this means a user will modify or update partial attributes, additional volitionally than all of them, in one modification.

In [11] A. Lewko and B. Waters propose a Multi-Authority Attribute-Based encoding (ABE) methodology. In this scheme, many parties will become ability and there's no

obligation for any public coordination except the development of a primary set of standard reference parameters. a celebration will primarily act as associate degree ABE authority by generating a public key and causing non-public keys to numerous users that replicate their attributes. A user will inscribe data in provisions of any Boolean formula over attributes send from each chosen set of authorities. At last, their system doesn't want any central authority.

J. Bethencourt give construction of a ciphertext-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 ciphertext if and as long as user's attributes pass all the means through the ciphertext's access formation [5].

3. Proposed System

Proposed system is used to provide high security to the confidential data shared among multiple objects. In first step,Key Authority(KA) generates the key for encryption and decryption of data and this key is sent to the commander. In second step, by using commander encrypts the data by using KA's key and his own Attribute Based Encryption (ABE). In third step, battalian decrypts the data. Experimental results show that proposed system is effective and more secure for real time information sharing in decentralized networks.

A

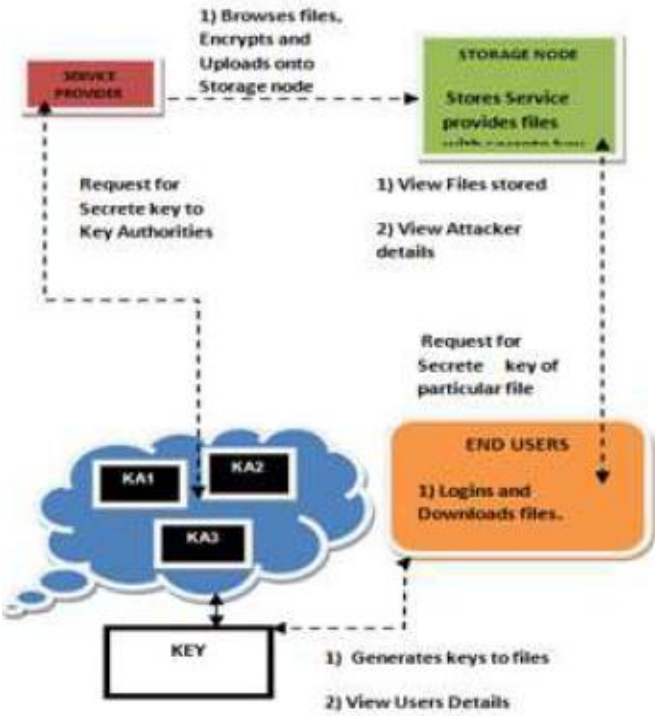

Figure: Block diagram of proposed system

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.

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.

4. 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 also, illegal access from the key authorities or storage 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.

In the circumstance of ABE, the backward secrecy wealth one user who that satisfies the access policy (i.e. who comes to hold an attribute) should be prohibited from bringing the plaintext of the preceding data exchanged before user holds the attribute. In contrast, forward secrecy wealth one user who drops an attribute should be prohibited from bringing the plaintext of the succeeding data altered subsequent to user drops the attribute, except the other convincing attributes that he is holding assure the access policy.

5. Mathematical Model

Set theory:
System S = {Input, Output}
Input:
For Commander:
Input = {Plain Text Message, Key generated Key Authority, Attributes}
Plain Text Message M = {M1, M2,..., Mn}

Attributes A = {A1,A2,...,An
For Receiver:
Input = {Encrypted Message, Key generated, Key Authority, Attributes}
Encrypted Message E = { E1, E2,...,En}
Attributes A = {A1, A2,...,An}
Output:
For Commander:
Output = {Encrypted Messages}={ E1, E2,...,En }
For Receiver:
Output = {Plain Text Messages}=f{M1, M2,...,Mn }
Constraint:
1] Commander and receiver should have valid attributes.
2] Commander and receiver should have key generated by key authority.

6. Algorithms

Our system uses two algorithms trippleDES and AES to provide high security to sensitive data.

7. Result Analysis

Developed system is very efficient in terms of performance, quality and security.

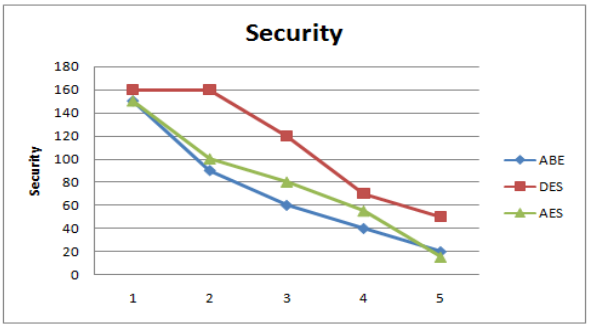

Figure: Security Graph

The above graph shows the developed system provides high security to the sensitive data.

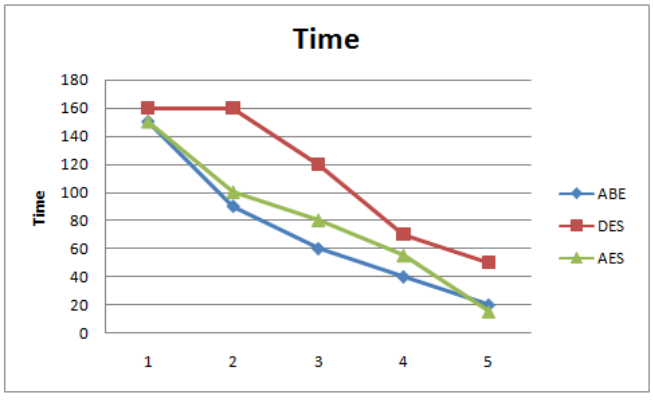

Figure: Time Graph

Graph shows system takes average time to produce expected Results.

8. Conclusion

High Secured attribute based system is proposed to provide high security for confidential data in organizations which contains sensitive data. We proposed a methods for providing security. In first step, the KA generates key using tripple DES algorithm. In second step, by using this KA's key and ABE commander encrypts the data. In third step, batalian decrypts the data and receive the message. Experimental results show that proposed system is effective and resourceful for real time applications to provide the security. We also demonstrate that this system can improve the performance significantly in the applications of data sharing.

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.
[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.

Author Profile

Snehal Gaikwad received the B.E. Degree in Information Technology in 2013, From Kolhapur Institute of Technology's College of Engineering , Kolhapur. Now, Pursuing M.E. Degree in Computer Engineering from KJ's College of Engineering & Management Research, Pune in current academic year 2015-16.