International Journal of Science Engineering and Advance Technology

Attribute Based Secure Military Data Retrieval System for Decentralized Disruption Tolerant Networks

Gubbala Siva Krishna [1], D.Ramesh [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: gubbalasivakrishna@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract—Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Key words: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), Secure data retrieval,multi authority, CP-ABE.

I. Introduction

For authentication, authorization and access control passwords are used. The password is selected by the user is predictable. This happens with both graphical and text based passwords. Users chooses memorable password, unfortunately it means that the passwords follow the predictable patterns that are very easy for guessing to the attacker. While allowing passwords to the user randomly the usability issues occurs, means user cannot remember the random passwords. There are number of graphical password systems has been developed; text-based passwords suffer with both security and usability problems. We well know that the human brain is better at remembering and recalling images than text, graphical passwords. The password method is very common method for the authentication purpose. This passwords used for safely login to emails over internet, sharing of data and transferring of files. Password causes some drawbacks like forgetting the password, very weak password or having less characters etc, So to secure the data and all application we have to provide a strong authentication as we using passwords in the military areas. So to provide high or strong authentication the new technique is introduced called as graphical password technique. The drawback of alphanumeric password is dictionary attack. So the graphical password technique improves the password techniques.

So the as an alternative to the alphanumeric password graphical password technique is used. As human brain can capable of remembering the images, pictures so this technique is designed to overcome the weakness and drawbacks of the traditional technique. The main drawbacks for the current graphical password schemes are the shoulder

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. For example, suppose that attributes “role 1” and “region 1” are managed by the authority A, and “role 2” and “region 2” are managed by the authority B. Then, it is impossible to generate an access policy ((“role 1” OR “role 2”) AND (“region 1” or “region 2”)) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as “-out-of-” logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

II. Related Work

ABE comes in two flavours called key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encrypt or only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user’s key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encrypt or, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encrypt or such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

1) Attribute Revocation:

Bettencourt*et al.* and Boldyreva *et al.* first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute

an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a ciphertext is encrypted with a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with. After time, say, a user newly holds the attribute set. Even if the new user should be disallowed to decrypt the ciphertext for the time instance, he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time , he can still decrypt the ciphertext of the previous time instance unless the key of the user is expired and the ciphertext is reencrypted with the newly updated key that the user cannot obtain. We call this uncontrolled period of time windows of vulnerability.

The other is the scalability problem. The key authority periodically announces a key update material by uncast at each time-slot so that all of the none revoked users can update their keys. This results in the "1-affects" problem, which means that the update of a single attribute affects he wholeno revoked users who share the attribute. This could be a bottleneck for both the key authority and all no revoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here).

However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead group elements1 additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bettencourt*et al.*, where is the maximum size of revoked attributes set. Golle *et al.* also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size.

2) Key Escrow:

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase *et al.* presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases and requires each user to store additional auxiliary key components besides the attributes keys, where is the number of authorities in the system.

3) Decentralized ABE:

Huang *et al.* and Roy *et al.* proposed decentralized CP-ABE schemes in the multiauthority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multiencrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively. Then, the only access policy expressed with is , which can be achieved by encrypting a message with by , and then encrypting the resulting ciphertext with by (where is the cipher text encrypted under), and then encrypting resulting ciphertext with by , and so on, until this multiencryption generates the final ciphertext . Thus, the access logic should be only AND, and they require iterative encryption operations where is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs. Chase and Lewko *et al.* proposed multiauthority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

B. Contribution

In this system, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encrypt or can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically

enforced against any curious key authorities or data storage nodes in the proposed scheme.

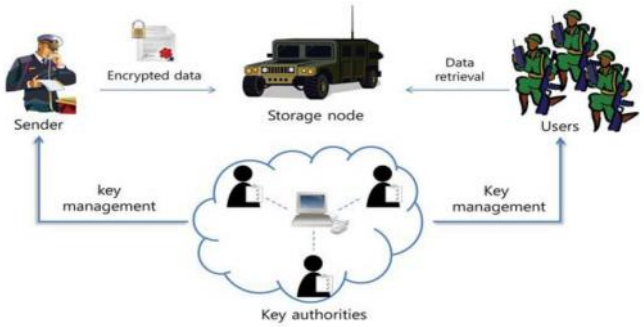


Fig 1: Architecture of secure data retrieval in a disruption-tolerant military network.

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

2) Collusion-resistance: If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

III. Problem Statement

The problem of a system is to maintain secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

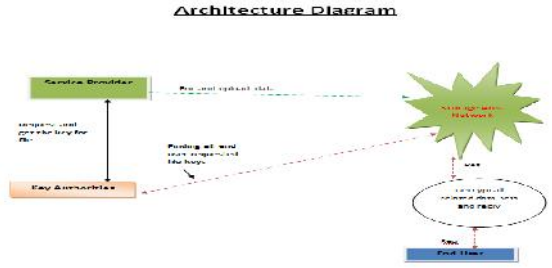


FIG:2 Architeture Diagram

IV. Modules For Development

B. User Module:

Sender: In this module, the Sender is responsible for registering the Users by providing details Name, Password, Confirm Password, Battalion (b1,b2,b3), Region(R1,R2,R3). Sender Browses the data File, encrypts it and gets the key from Key Authority Server (KA1, KA2, and KA3). Uploads their data files to the Storage Node and sender is authenticated to provide privileges for End User.

Disruption Tolerant Network Router: The Disruption Tolerant Network Router (DTN) technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. In this module we introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. In DTN encrypted data file and details will be stored Storage Node.

Key Authority: The key authority (KA1, KA2, and KA3) is responsible to generate the secret key for the file belongs to the particular Battalion and region. The End User Request to the storage node using the file Name, secret key, Battalion and Region, Then storage node connect to the respective Key authority server. If all specified Details are correct then file will sent to the end user, or else he will be blocked in a storage node. The Key Authority server can view the users, privileges, keys. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

End User: In this module, the End user can access the file details and end user who will request and gets file contents response from the DTN Router. If the credential file name and secret key is correct then the end user will get the file response from the router in Decrypted format.

Threat model: Threat model is one who is trying to access the file which is belongs to other user by injecting the fake details to the file in the storage node is considered as Attacker. The attacker can be Data confidentiality or collusion-resistance.

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
2) Collusion-resistance: Suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users keys.

V. Functional And Non Functional Requirement Specification:

This Chapter describes about the requirements. It specifies the hardware and software requirements that are required in order to run the application properly. The Software Requirement Specification (SRS) is explained in detail, which includes overview of this dissertation as well as the functional and non-functional requirement of this dissertation.

SRS for Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Functional	Control the Congestion in DTN Router; Key generation, Authenticate the users, multiauthority in key authority server for key generation, Providing the access control for each and every file by generating the keys, Protects the Files in disruption-tolerant network, secure data retrieval, Finding the malicious user.
Non- Functional	The Sender and Receiver never Find the Router performance.
External interface	LAN , Routers, WAN
Performance	Finding File Attackers Information, Access control of files in network, View the Privileges, Viewing the keys, View the Registered user, authentication of a user, Encrypt the contents, attribute based encryption, End User Can view files available.
Attributes	File Management, Attackers, Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority and secure data retrieval.

Table: 3.1 Summaries of SRS

Functional Requirements

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

- The Service provider /Sender are responsible for registering the Users by providing their details, including Battalion and Region.
- The Service Provider/Sender Browses the data File, encrypts it and generates the key from Key Authority Server (KA1, KA2, and KA3) and uploads file to the destination.
- The DTN Router stores the encrypted data file and their details in the Storage Node.
- The End User Request to the storage node using their credentials like file Name, secret key, Battalion and Region.
- Then storage node connects to the respective Key authority server. If all credentials are correct then user is authorized to receive the file.
- If the user gives wrong credentials file name, secret key, Battalion, Region, then the end user will considered as non authorized user.
- The Attributes are File Management, Attackers, Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

Non – Functional Requirements

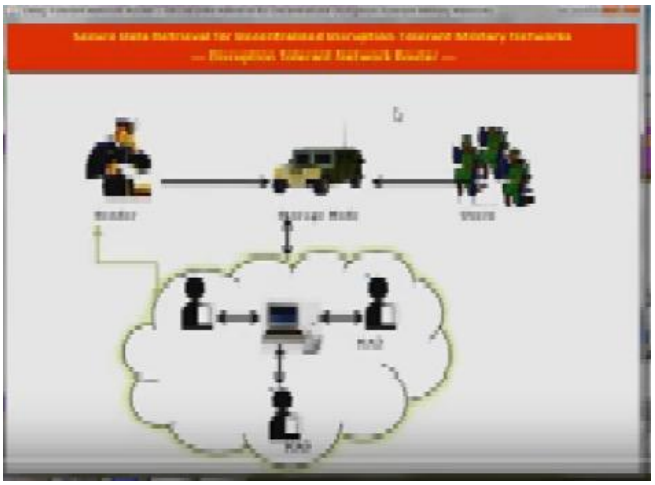
Non – Functional requirements, as the name suggests, are those requirements that are not directly concerned with the specific functions delivered by the system. They may relate to emergent system properties such as reliability response time and store occupancy. Alternatively, they may define constraints on the system such as the capability of the Input Output devices and the data representations used in system interfaces. Many non-functional requirements relate to the system as whole rather than to individual system features. This means they are often critical than the individual functional requirements. The following non-functional requirements are worthy of attention.

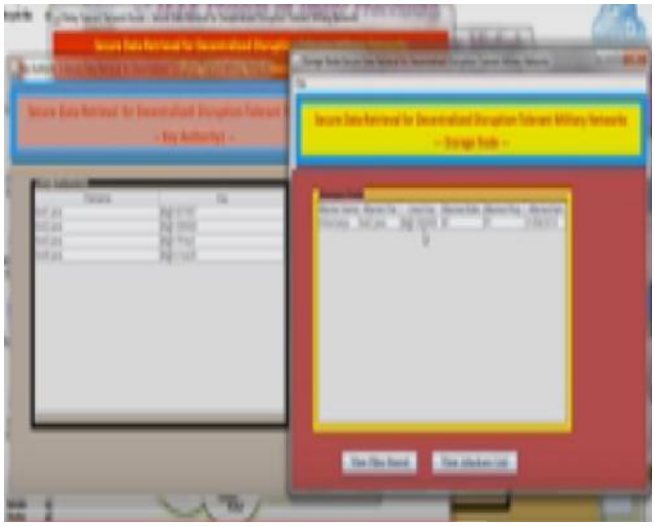
The key non-functional requirements are:

- Security: The system should allow a secured communication between Sender and Router and Receiver.
- Energy Efficiency: The Time consumed by the Router to transfer the File's Packets from the Receiver.
- Reliability: The system should be reliable and must not degrade the performance of the existing system and should not lead to the hanging of the system.

Results

Screen Shots:





VI.Conclusion

We have proposed a novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach this system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network

VII.Acknowledgment

It is my pleasure to express sir Mr. H. D. Sonawane, Computer Engineering, BVCOE&RI, and continues support. This paper could not be success without my knowledge to my respected secure algorithm done Nashik for his valuable guidance, inspiration which help to understand the necessity for this paper.

References

[1] 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.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing schemefor disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route designfor sparse ad hoc networks with mobile nodes," in *Proc. ACMMobiHoc*, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policyattribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-basedinformation retrieval schemes for DTNs," in *Proc. IEEE MILCOM*,2007, pp. 1–7.

[6] 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.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application,"in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective groupbroadcast in vehicular networks using dynamic attribute based encryption,"in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcementin vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8,pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.Eurocrypt*, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in *Proc.ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebasedencryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp.321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryptionwith non-monotonic access structures," in *Proc. ACM Conf. Comput.Commun. Security*, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharingwith attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryptionwith efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*,2008, pp. 417–426.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebasedsystems," in *Proc. ACMConf.*