NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 10, Oct. -2017

SECURELY DATA RETRIEVAL FOR DECENTRALIZED DISRUPTION TOLERANT MILITARY SYSTEMS

RHATAVAL AVADHUT DHONDIRAM
ME E&TC BVCOE Kolhapur, E-mail: avadhut.rhataval@gmail.com

PROF. DR. K. R. DESAI
Guide, Department of E&TC, Bharati Vidyapeeth College of Engineering, Kolhapur.

ABSTRACT:

There are some parts of the military environment, such as battlefields or hostile areas. They may suffer from intermittent network connections. They have frequent partitions. Networking DTN networking technology is a truly simple solution. DTN network, tear-resistant; it allows wireless and military personnel to carry the interaction with each other. These devices reliably protect confidential information or use external storage node commands. In these network environments, DTN is a very successful technology. If there is no wired connection between the source and the target device, the intermediate node may need information from the source node for a long time until the connection is properly established. One of the complex methods is ABE. This is a property-based encryption that meets the requirements for secure data retrieval in DTN. This concept is a password strategy Cipher text-Policy ABE (CP-ABE). It provides an appropriate way to encrypt data. Encryption includes a set of attributes that need to be decrypted to decrypt the encrypted text. Therefore, many users can be allowed to decrypt different data according to the security policy.

KEYWORDS: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure

INTRODUCTION:

In many military networks, the connection of wireless devices shipped by soldiers may be temporarily disabled due to interference, environmental factors and mobility, especially when working in harsh environments. The failover network (DTN) interrupt technology is a successful solution that allows nodes to communicate with each other in these extreme network environments. Typically, when there is no end-to-end connection between the source node and the destination node, the communiqué from the source node may take a long time on the intermediate node until the connection is finally established. Encryption based on the Cyper Text Policy (CP-ABE) attribute is a promising encryption solution for access control. However, the use of CP-ABE in decentralized DTNs poses a number of security and privacy issues regarding recall properties, storage keys, and coordination of various rights issues. We propose a secure data extraction scheme for a distributed DTN using CP-ABE, where the organization with multiple keys manages its attributes. We demonstrate how to apply the proposed mechanism to safely and effectively manage confidential data distributed in a fault-tolerant military network to illustrate the benefits of using this approach.

PROBLEM DEFINATION:

Military applications should increase the protection of confidential data, including access control methods. In many cases, it is desirable to provide differentiated access services, so that the data access policy is defined as an attribute or user role that is managed by the primary privilege. Based on a joint analysis of visual content and additional information, the D2C2 algorithm is proposed for detecting visual images. The content set is divided into subsets based on additional information, and unique and common visual patterns are detected by several stages of learning and clustering of several instances that are analyzed inside and within these subsets. This mode helps visualize the contents of data and generate lexical functions for semantic classification. The proposed structure is quite general and can handle all types of information outside the game and combines various common / unique templates extraction algorithms. The future work is to improve the joint generation, emphasizing the consistency of sharing, rather than the current heuristic clustering. Another future work is to use unique shared templates to study other applications without needing to define them. If this is not inevitable, do not use abbreviations in headings or titles.

LITERATURE REVIEW:

Mobile units in military conditions, such as battlefields or hostile areas, may suffer from intermittent network connections and frequent separation. The interrupted technology of a fail-safe network (DTN) is a successful solution allowing soldiers to transfer wireless devices to communicate with each other and reliably receive confidential information or commands using external storage nodes. In this case, some of the most

difficult problems are the use of an authorization strategy and the update of the search strategy for security data. Encryption based on encrypted text policy attributes (CP-ABE) is a promising encryption solution for access control. However, the use of CP-ABE in a decentralized DTN introduces many security and privacy concerns in terms of recalling attributes, storing keys and coordinating various releases of rights [1].

The Wireless Sensor Network (WSN) is based on detecting the basic sensor that occurs in certain areas of the monitoring area. In the most recent critical WSN application, you can find applications for monitoring borders. The first goal of such an application is to monitor the country's borders and detect the presence of intruders near the border. In this article, we have theoretically studied the effects of natural factors on the dynamic deployment of a hierarchical WSN solution that provides two observation lines. The parameters of the wind, altitude, and speed of the aircraft emitted by the sensor are entered into the equation for optimizing the coverage area and the WSN connection. We then provide a mathematical model to evaluate the quality of the connection and coverage of the deployed network and allow planning and determining the size of the boundary solution [2]-[3].

Barrier coverage of wireless sensor networks is designed to detect intruders throughout the network. It provides a viable alternative to monitoring border borders, national borders, coastlines and the boundaries of critical infrastructures. Early studies of barrier coating usually assume that the sensors are deployed over a large area in a random and even manner. This assumption, if it is theoretically interesting, can be impractical in practical applications. We are using a more realistic approach in this article. In particular, we believe that the sensor flew the aircraft from the aircraft. We note that wind, geographic landscape, and other factors can lead to a random displacement of the sensor from the place of its target landing point. Therefore, it is more realistic to assume that the sensor nodes are distributed along the deployment line with normal displacements [3]-[5].

MOTOVATION:

We provide a multipurpose CP-ABE scheme for distributed secure data retrieval in the DTN. Each local authority handles some personalized and critical components to the user through a secure protocol 2PC with the central authority. Each user attribute key can be updated individually and immediately. As a result, the proposed scenario can improve scalability and security. Since the first CP-ABE program proposed by Bethencourt et al. [13] proposed schemes tens CP-ABE [7], [21] - [23]. Subsequent program CP-ABE is mainly carried out through the standard model more rigorous proof of safety. However, most programs do not correspond to the expressiveness of the program Bethencourt et al.

The main priority to resolve following issues in proposed Project as:

1. Key Escrow
2. Decentralized ABE Scheme
3. Central authority and local authority take part with MD5-Algo which prevents to identify them each other main Secrets.
4. User should not revoked its attributes and satisfying access policies
5. Sender is accountable for enforcing access scheme

PROPOSED METHOD:

1) Key Authorities: These are the key creation centers for generating common/secret parameters for CP-ABE. It mainly consists of the central government and local authorities. We assume that there is a reliable and trustworthy channel of communication between central authorities and local authorities in the early stages of creating and creating keys.

Each local privilege handles different attributes and issues a corresponding user key. They provide access to different users based on user characteristics. The main principles are considered sincere but strange. That is, they will honestly perform the tasks assigned to the system, but they want to learn the encrypted content information as much as possible.

2) Storage node: This is an entity that stores data from the source and make available corresponding access to the consumer. It may be gesticulation or static. Similar to the previous scenario, we also assume that the storage node is semi-reliable, which is genuine but curious.

3) Sender: This is an entity that holds trustworthy messages or data and wants to store them in an external data storage node for easy sharing or sending to users in an end-to-end environment. The sender is responsible for defining the access policy (attribute) and enforcing its own data by encoding the policy data before storing the policy data in the storage node.

4) User: This is a mobile node who wants to right to use the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the right to use policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the IDEA algorithm and obtain the data. Since key authority is semi-reliable, they must block access to the node data; they can also issue a key to the user. In order to realize this somewhat contradictory requirement, the enteral authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. 2PC protocol prevents them

from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually.

METHODLOGY:

We propose a security-based data retrieval system that uses CP-ABE's distributed DTN. The proposed program achieves the following achievements. First, by reducing the vulnerability of the window to enhance the confidentiality of confidential data, the direct function is revoked. Second, the encoder can define fine access policies using any monotonic access structure based on the attributes issued by any selected set of permissions. Third, the use of distributed DTN architecture features non-prototype key distribution protocol to solve the key escrow problem. The key release protocol creates and publishes the user key by running the 2PC security protocol between the original permissions and has its own master password. The 2PC protocol prevents raw permissions from getting information between master keys so that they cannot create a set of user keys separately.

As a result, users do not need to fully trust authorities to protect their data from sharing. Privacy and data privacy can be performed on any strange central organization or data storage node in the proposed scenario.

CONCULSION:

Technology is a successful solution for military applications that allows wireless devices to communicate with each other and reliably access confidential information by using external storage nodes. This is an extensible encryption solution for accessing control issues and secure data retrieval issues. In this paper, we present an efficient and secure method of using this decentralized DTN method to recover data, many of which are independently managed by its own attributes. Resolve inherent key escrow issues to ensure the confidentiality of stored data, even in hostile environments where potential principles may be threatened or not fully confident.

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 scheme for disruption tolerant networks*," in Proc. IEEE MILCOM, 2006, pp.1–6.
3) 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.
4) 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.
5) M. Chuah and P. Yang, "*Performance evaluation of content-based information 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, "*Mediated ciphertext-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 group broadcast 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 enforcement n vehicular ad hoc networks*," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.
10) Lewko and B. Waters, *"Decentralizing attribute-based encryption,"* Cryptology Print Archive: Rep. 2010/351, 2010.
11) Sahai and B. Waters, *"Fuzzy identity-based encryption*," in Proc. Euro crypt, 2005, pp. 457–473.
12) V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for 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 attributebased encryption,*" in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
14) R. Ostrovsky, A. Sahai, and B. Waters, "*Attribute-based encryption with 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 sharing with attribute revocation,"* in Proc. ASIACCS, 2010, pp. 261–270.