IJCTA, 10(01), 2017, pp. 31-37

Analytics of Efficient Data Controller in Cloud Computing

K. Nithya* and X. Nancy*

Abstract : The main aim is to analyze the security through Best Peer++. There is a corporate network storage node called Disruption Tolerant Networking (DTN) that allows users for storing, retrieving and sharing information. DTN is the most successful solution for the military networks, because it works even in the extreme networking environment. The captain needs to store some data into the DTN storage node, the data can be accessed within the soldiers. The problems with the existing system is, the third parties can able to hack the message stored in the storage node, by creating, modifying and deleting the message. The problem occurs during the encryption, the third parties can able to encrypt the sender's message with the help of sender's public key, then he creates a duplicate message and re encrypt it to the receiver. The receiver receives the duplicate message and believes that the message was sent by the sender. In order to the overcome such problems, we propose some encryption techniques and algorithms that are used to secure data. BestPeer++, a system which delivers extendible data sharing services for communal network applications in the cloud.

Keywords :

1. INTRODUCTION

In many army network scenarios, connections of wire-less devices carried by soldiers may be temporarily disconnected by crashing, environmental factors, and mobility, especially when they operate in unsociable environments. Disruption tolerant network (DTN) technologies are enhancing successful solutions that allow nodes to advertise with each other in these supreme networking environments. Mostly, when there is no point-to-point connection between a sender and a receiver pair, the messages from the sender node may need to wait in the in-between nodes for a stable amount of time until the connection would be established eventually.

Roy and Chuah brought out storage nodes in DTNs where the data is stored or imitated such that only valid mobile nodes can use the necessary information quickly and efficiently. Many army applications are in need of secured confidential data including access control techniques that are cryptographically required. In several cases, it is desirable to provide various access services such that accessing data policies are defined over roles and attributes of user, that are managed by the key in-charges. For example, in a disruption-tolerant army network, a commander may store confidential information at a storage node, which have to accessed by members of

"Battalion 1" who are all participating in "Sector 2."

Here, it is a justifiable assumption that more than one key authorized person's are likely to handle their own dynamic attributes for commando's in their implemented sectors or echelons, which could be periodically changed (*e.g.*, the attribute showing current region of moving commando's). We taken a reference to this DTN architecture where more than one authorized person's issue and handle their own attribute keys independently as a decentralized DTN.

* Assist. Prof , Department of CSE, Veltech Multitech Dr.RR Dr.SR Engg College, Chennai, *nithyakcse@veltechmultitech.org, nancy@veltechmultitech.org*

2. EXISTING SYSTEM

In many army network scenarios, connections of wireless devices carried by fighter's may be temporarily disconnected by crashing, fortuitous factors, and mobility, particularly when they operate in unfriendly environments. Disruption- tolerant network (DTN) methodologies are becoming outstanding solutions that allow nodes to interact with each other in these extreme networking environments. Typically, when there is no point-to-point connection between a sender and a receiver pair, the messages from the sender node may need to wait in the intermediate nodes for a valuable amount of time until the connection would be eventually established. Mr. Roy and Mr. Chuah imported storage nodes in DTNs where data is stored or duplicated such that only authorized mobile nodes can operate the necessary data quickly and efficiently Many army applications needed increased protection of confidential data including access control methodologies that are cryptographically enforced.

In various cases, it is appropriate to provide various access services such that information access policies are defined over user attributes or roles, which are handled by the key authorities. -For example, in a disruption-tolerant army network, a commander may store a confidential data at a storage node, which should be accessed by members of "armed forces 1" who are participating in "sector 2." In this case, it is a valuable Presumption that multiple key authorities are likely to handle their own dynamic attributes for commando's in their implemented regions or echelons, which could be continuously changed (*e.g*., the attribute Pointing current region of moving soldiers).

1. The captain (sender) is the admin who sends the messages directly to the soldiers (receivers).
2. The soldiers will follow the captain's message accordingly.
3. The captain's public key is visible to the soldiers.
4. The third parties such as hackers can easily encrypt the captain's message, with the help of captain's public key.
5. Then he creates a duplicate message and re–encrypt it to the soldiers.
6. The soldiers will receive the duplicate message sent by the hacker.
7. The soldiers believe that the message was sent by the sender and follows accordingly.

Limitations of Existing System

1. Loss of data during encryption.
2. No proper security is established.
3. No Proper Encryption Schema is implemented.
4. There is no private key facility for both sender and receiver.

3. PROPOSED SYSTEM

The goal of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data come back in DTNs. ABE features a mechanism that enables an access control over encrypted data using access methods and characterized attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable manner of encrypting data such that the encryptor defines the attribute set that the decryptor have to possess in order to decrypt the cipher text. Thus, various users are granted to decrypt various pieces of data as per the security policy. However, the trouble of applying the ABE to DTNs introduces various security and confidential challenges. Since few users may modify their correlated attributes at some point (for instance, moving their region), or some private keys might be negotiated, key revocation (or update) for each attribute is fundamental in order to make systems protected. However, this concern is even more difficult, especially in ABE systems, since each attribute is conceivably shared by many users (henceforth, we specify to such a collection of users as an attribute group). This signifies that revocation of any attribute or even a single user in an attribute group would

disturb the other users in the group. For instance, if a user adds or quits an attribute group, the coordinated attribute key should be modified and redistributed to all the other users in the same group for behind or ahead secrecy. It may result in congestion during rekeying method, or security weakening because of the windows of vulnerability if the previous attribute key is not changed instantly. one more problem is the key escrow problem.

In CP-ABE, the key authority creates private keys of users by using the authorized users master secret keys to users' coordinated set of attributes. Thus, the key in-charge can decrypt every encrypted text addressed to specific users by creating their attribute keys. If the key in-charge is adjusted by attacker when deployed in the unsociable environments, this could be a potential hazard to the data confidentiality or privacy specifically when the data is more sensitive. The key is an fundamental issue even in the multiple-authority systems since each key authority has the entire rights to create their own attribute keys with their own master secrets. As long as such a key generation technique based on the single master secret is the primitive method for most of the asymmetric encryption systems such as the attribute-based or identity-based encryption protocols, deleting escrow in single or multiple-authority CP-ABE is a pivotal open problem.Huffman Coding Greedy Algorithm is used for the preventing the loss of data 3 during the encryption process.In the proposed system there aretwo local cloud servers using Best Peer ++. One is for storing user's data and messages.Other is for managing public key and private key for both sender and receiver.There is a separate private key for both captain (sender) and soldiers (receivers). Best Peer ++ integrates cloud computing, database, and P2P technologies into one system[2] [5], that provides an ultimate security for the users.

4. HUFFMAN CODING - A GREEDY ALGORITHM

Greedy Algorithms

A **greedy algorithm** is an algorithmic paradigm that follows the problem solving heuristic of making the locally optimal choice at each stage with the hope of finding a global optimum. Build solutions with small decision

The Task at Hand

Encoding symbols using bits Suppose we want to represent symbols using a computer.

1. Letters of the English alphabet (or more broadly ASCII characters).
2. Pixels of an image.
3. Audio information from a sound clip. Ultimately these are converted to bits.

Types of Codes that can be used to represent symbols

Fixed length codes

1. Every symbol is encoded using an Equal number of bits
2. E.g. ASCII code 256 symbols Encoded using 8 bits

A = 01000001
! = 00100001
8 = 00111000
q = 01110001

Decoding

1. Simply chop the data into blocks of 8 bits each and decode one symbol for each block.

5. FIXED LENGTH CODES [FLC]

1. Every symbol is encoded using an equal number of bits

2. E.g. color image pixels – most consumer cameras generate 24-bit color images
   8 bits for Red
   8 bits for Green
   8 bits for Blue

If a 8-Megapixel image isn't compressed,
it requires 24 Megabytes for storage!

6. LETTER PROBABILITIES IN THE ENGLISH ALPHABET

Table 1

Letter Probabilities in the English Alphabet

Symbol	*Probability*	*Symbol*	*Probability*
Space	0.1859	N	0.0574
A	0.0642	O	0.0632
B	0.0127	P	0.0152
C	0.0218	Q	0.0008
D	0.0317	R	0.0484
E	0.1031	S	0.0514
F	0.0208	T	0.0796
G	0.0152	U	0.0228
H	0.0467	V	0.0083
I	0.0575	W	0.0175
J	0.0008	X	0.0013
K	0.0049	Y	0.0164
L	0.0321	Z	0.005
M	0.0198		

VARIABLE LENGTH CODES [VLC]

Assign shorter code words to more frequent symbols, longer code words to less frequent symbols

Tabel 2

Variable Length Codes

Symbol	*Probability*	*Code I*	*Code II*	*Code III*
A	0.60	00	0	0
B	0.30	01	1	10
C	0.05	10	10	110
D	0.05	11	11	111

PROBLEM WITH CODE II

1. Suppose we receive the encoding: 11011.
2. Is that "BBABB" or "BCD" or "DAD" or …
3. Code II is not **uniquely decodable.**

CODE III

Code III is a **prefix-free** variable length code

1. Somewhat confusingly, we will refer to this as a **prefix code.**

2. No codeword is a prefix of any other codeword.
3. Prefix codes are uniquely decodable.

7. OPTIMAL PREFIX CODES [OPC]

Among all possible prefix codes, can we devise an algorithm that will give us an optimal prefix code.

One that most efficiently encodes the symbols with the lowest average bits per symbol. Huffman codes are optimal prefix codes. Each leaf node represents a symbol. Each path represents an encoding for that symbol.

Traveling to the left child is a '0'.

Traveling to the right child is a '1'.

For a symbol to a prefix of another, it would have to be a non-leaf.

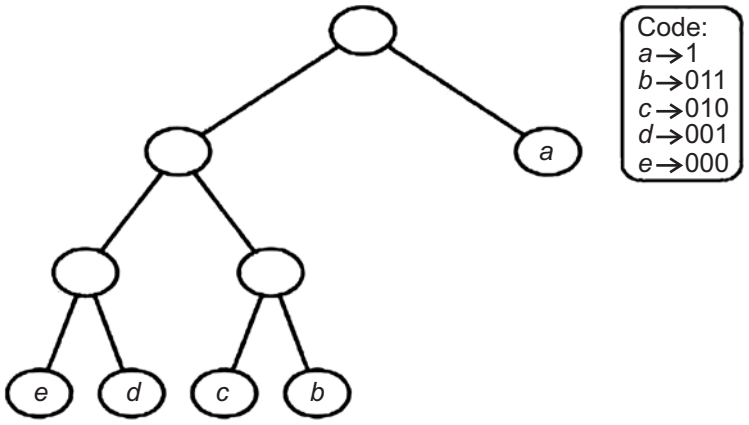

Figure 1: Optimal Prefix Code I

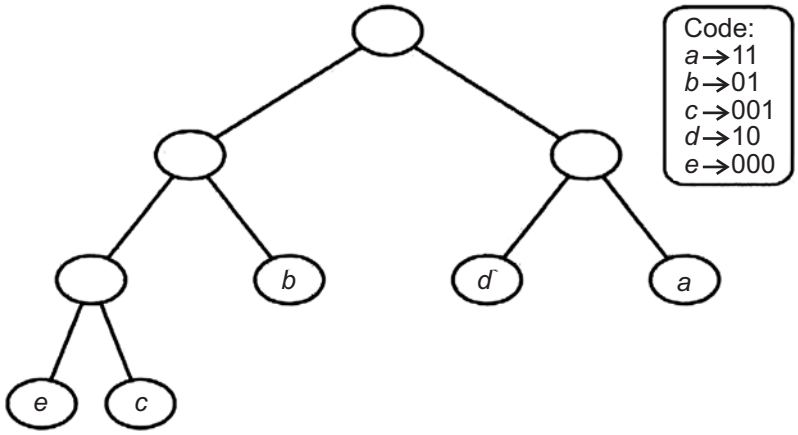

Figure 2: Optimal Prefix Code II

The above three diagrams depict the three different prefix codes for the alphabet S= {*a*,*b*,*c*,*d*,*e*}.

8. THE HUFFMAN CODING ALGORITHM GENERATES A PREFIX CODE (A BINARY TREE)

Overall idea – bottom-up approach

1. Start with all symbols as leaf nodes
2. Associate with each symbol its frequency of occurrence
3. REPEAT until only one symbol remaining.

Select the two least frequently occurring symbols and link them together as children of a new common parent symbol.

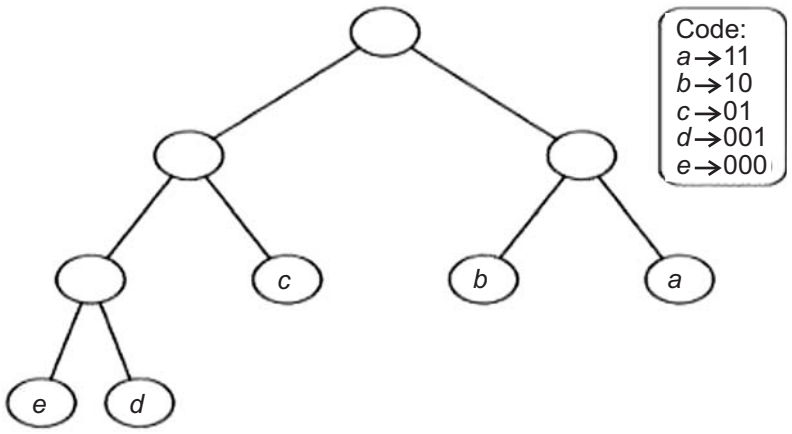

Figure 3: Optimal Prefix Code II

Associate with this new parent symbol the combined frequency of the two children. Remove the children from the collection of symbols being considered and replace with the new parent symbol.

Each step introduces a new parent symbol but removes two children.

Each step is building the tree from the leaves up to the root.

Code words for each symbol are generated by traversing from the root of the tree to the leaves.

Each traversal to a left child corresponds to a '0'.

Each traversal to a right child corresponds to a '1'.

9. METHODOLOGY

HUFFMAN CODING - A GREEDY ALGORITHM

Build up solutions in small steps.

Make local decisions.

Previous decisions are never reconsidered.

GREEDY–HUFFMAN ALGORITHM (C)

1. $n \leftarrow |C|$
2. $Q \leftarrow C$
3. for $i \leftarrow 1$ to $n - 1$
4. do $z \leftarrow$ ALLOCATE–NODE()
4. $x \leftarrow$ left[z] $\leftarrow$ EXTRACT–MIN(Q)
6. $y \leftarrow$ right[z] $\leftarrow$ EXTRACT–MIN(Q)
7. $f[z] \leftarrow f[x] + f[y]$
8. INSERT(Q, z)
9. **return** EXTRACT-MIN(Q)

Advantages of Proposed System

Data Transmission without any interruption. Secure transmission of data between nodes. Prevents loss of data during encryption.

10. CONCLUSION

DTN technique are becoming best solutions in army applications that allow wireless devices to interact with each other and access the confidential data accurately by handle external storage nodes. CP-ABE is

a reliable cryptographic solution to the access control and secure data retrieval issues.Here , we suggested an efficient and secure data retrieval technique with the help of CP-ABE for decentralized DTNs where more than one key authorities handle their attributes independently and using Huffman Coding Greedy Algorithm for preventing loss of information during the encryption process. The inherent key guarantee problem is resolved such that the confidentiality of the stored data is guaranteed even under the unfavorable environment where key authorized Person's might be com-promised or untrustworthy Here we recommended, the fine-grained key revocation can be done for each attribute group. We indicate that, how to apply the suggested part to securely and efficiently handle the confidential information scattered in the disruption-tolerant army network. Thus the Best Peer++ is a promising solution for efficient data sharing within corporate networks.

11. REFERENCES

1. Ning Cao, Cong Wang, Ming Li, KuiRen and Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data" pp: 222-233 Issue No.01 Vol.25 – Jan- 2014
2. H.V. Jagadish, B.C. Ooi, K.-L.Tan, Q.H. Vu, and R. Zhang, "Speeding up Search in Peer-to-Peer Networks with a Multi-Way Tree Structure,"Proc. ACM SIGMOD Int'l Conf. Management of Data, 2006.
3. Adnan Tariq, Boris Koldehofe , University of Stuttgart, Stuttgart, Kurt Rothermel "Securing Broker-Less Publish/ Subscribe Systems Using Identity-Based Encryption" Vol.25 pp: 518-528 Issue No.02 – Feb-2014
4. MatteoSerenoDipt. di Inf., Univ. di Torino, Turin, Italy "Rateless Codes and Random Walks for P2P Resource Discovery in Grids" pp: 1014-1023 Issue No.04 - Vol.25 April -2014.
5. H.V. Jagadish, B.C. Ooi, and Q.H. Vu, "BATON: A Balanced Tree Structure for Peer-to-Peer Networks," Proc. 31st Int'l Conf. Very Large Data Bases (VLDB '05), pp. 661-672, 2005.
6. A. Lakshman and P. Malik, "Cassandra: Structured Storage System on a P2P Network," Proc. 28th ACM Symp. Principles of Distributed Computing (PODC '09), p. 5, 2009.
7. W.S. Ng, B.C. Ooi, K.-L. Tan, and A. Zhou, "PeerDB: A P2P-Based System for Distributed Data Sharing," Proc. 19th Int'l Conf. Data Eng., pp. 633-644, 2003.