International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Securing and Low Time Consuming for Sharing High Sensitive and Relevant Data

Princy .B[1], Nishley Elizabeth Joseph[2]

[1]M. Tech Student, Marian Engineering College, Trivandrum, Kerala, India

[2]Assistant Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India

Abstract: ***The wireless medium in the military networks are not able to transfer the confidential data between the commander and the soldiers. The commander sends the information to the storage node after encrypting with the help of private keys provided by the key authorities. The soldiers retrieve the information from the storage node by providing their details to the multiple key authorities they provide a private key which helps them to decrypt the information from the storage node.CP-ABE scheme is used for retrieving and securing their data. For data encryption and decryption scalability is provided by ABE.But the problem is that key authorities cannot be fully trusted because they can also access the data from the storage node with the private keys provided by them.In this paper, I demonstrate how to apply the proposed scheme inSecuring and Low Time Consuming for Sharing High Sensitive and Relevant Data.***

Keywords: Access control,Attribute based encryption, Multiauthority, SecureData Retrieval, Networks

1. Introduction

In many military environment is a hostile and a turbulent one, applications running in this environment needs more security to protect their data. CP-ABE based encryption provides fine grained access control. Military applications require protection for the confidential data which includes the access control methods that are enforced cryptographically.Each user is associated with a set of attributes and generated based upon the private key. Contents areencrypted under an access policy and for decryption those users' attributes should match the access policy. For example, in a military network; the confidential information's are stored at the storage node by the commander and it can be accessed by the members of a particular group (name of the group will be given e.g.: Battalion 1)and those who are in a particular region (name of the region is given e.g.: Region 2).The dynamic attributes are managed by the multiple key authorities for soldiersbased on the regions which could change frequently (e.g., the attribute taken is the current location of the soldier). The DTN architecture where multiple authorities issue and manage their own attribute keys independently.

The concept of attribute-based encryption (ABE) is an approach that fulfills the requirements for secure data retrieval. ABE is a mechanism which enables an access control over encrypted data using access policies and ascribed attributes among private keys. The key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node they are still able to issue secret keys to users. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. However, this issue is even more difficult, especially when the multiple users share each attribute conceivably in ABE system

In the securing of data with low consuming time we use different methods based upon the information. The first method is the general method of encrypting the data, second the Strong hiding commitment scheme and finally a steganography process. This paper describes about securing the data and not able to retrieve the information by the key authorities.

2. Related Works

Securing of confidential information with low consuming time comes out in two flavors called steganography and secure data transfer. The Steganography is the art of hiding message in a carrier file (here in this paper we are using image as a carrier file) so that hidden message is not known to others. The concept of steganography is that message to be transmitted is not detectable to casual eye. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication.

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. It is motivated to satisfy the strong hiding property whilekeeping the computation and communication overhead toa minimum. The strong hiding property is satisfied by formatting the packet header, so that all bitsare modulated in the last few PHY layersymbols of the packet.

3. Proposed System

Proposed system focuses on secure for confidential data with low time consuming and providing different ways. Steganography is the first method applied for securing the confidential data.It is the practice of allowing a user to hide large amounts of information within an image. The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye.Hiding data in an image, then sending that image to someone else could also be considered

a covert channel.It is secure if it cannot be removed even with full knowledgeof the secret key.Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. After hiding the information in the image we are encrypting the whole image once again using the private keys provided by the key authorities. It is an advantage of securing the confidential information is to make the key authorities not to able to retrieve the information using the keys.

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. SHCS requires the joint consideration of the MAC and PHY layers. To achieve the strong hiding property, a sublayer called the "hiding sublayer" is inserted between the MAC and the PHY layer. For every packet m, a random key k of length s is appended. The computation overhead of SHCS is one symmetric encryption at the sender and onesymmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined.

4. Performance Analysis

The performance of the level based upon sharing high sensitive and relevant data and that can be security it provides. This software will provide high security without any information lossissue and can be used in any organization. The performance is analyzed based upon the comparing the three different methods used for securing the high sensitive relevant data.Different load have been used to determine the processing power and performance of each techniques

5. Conclusion

CP-ABE is considered to be the scalable cryptographic solution to the access control and securing data retrieval issues. In this paper, we proposed a secure and low time consuming methods such as steganography process for hiding the confidential information inside any media and strong hiding commitment scheme for satisfying by analyzing per packet computation and communication overhead. Confidentiality of the data is guaranteed under the hostile environment because before sending the date the sender confirms whether there is a receiver on the other hand to receive the information that is transferred or shared. We demonstrate how to apply the proposed mechanism to Securing and Low Time Consuming for Sharing High Sensitive and Relevant Data.

References

[1] JunbeomHur and Kyungtae Kang, Member, IEEE, ACM, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," IEEE Transactions on Networking vol:22 no:1 year 2014
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.
[3] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010
[4] S. Roy and. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.
[6] Alejandro proano and Loukaslazos "Packet-Hiding Methods For Preventing Selective Jamming Attacks" IEEE Transactions on Dependable and Secure Computing,vol. 9, no. 1, year 2012
[7] UmohBasseyOffiong, M. B. Mukeshkrishnan "Securing Data Retrieval for Decentralized Disruption-Tolerant Military Networks (DTNs) using Cipher text-Policy Attribute-Based Encryption" International Journal of Engineering Trends and Technology (IJETT) – Volume 26 Number 5- August 2015
[8] Niranjana Devi S, Senthilnathan K "Secure Data Retrieval Scheme Based Cipher text -Policy Attribute Based Encryption (CP-Abe) System For Decentralized Disruption Tolerant Military Networks" International Journal of Emerging Technology & Research Volume 1, Issue 7, Nov - Dec, 2014