International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 79 - 80

High Sensitive and Relevant Data Sharing with Secure and Low Time Consuming

Princy.B[1], Nishley Elizabeth Joseph[2]
M. Tech Student, MarianEngineeringCollege, Trivandrum, Kerala, India[1]
Asst. Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India[2]

Abstract:-Intermittent connection of networks and partition taken place frequently are likely to be suffered in military environments. Wireless devices are enabled in the network for accessing the confidential data with security by utilizing the storage nodes and alsothere is a communication with each other.Several privacy challenges andsecurity is based upon the attribute revocation and coordination of attributes issued from differentauthorities independentlywhich are introduced by the ABE scheme.For data encryption and decryption scalability is provided by ABE. In the case of encrypting the data, it is encrypted using certain polices and the attributes based upon the private keys and for decrypting the data it must possess some attributes that must match with the security policy that is applied in the particular data. The confidentiality of the stored data evenin the hostile area where key authorities are not fully trusted. In this paper, we demonstrate method of applying the proposed scheme in high sensitive and relevant data sharing with secure and low time consuming.

Keywords*:Access control,Attribute-Based Encryption (ABE), Multiauthority, SecureData Retrieval.*

*****

I. 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 soldiers based 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 hiding scheme, third method is matrix method and finally a steganography process. This paper describes about securing the data without the help of key authorities.

II. RELATED WORKS

Securing of confidential information with low consuming time comes out in two flavors called stegnography and secure data transfer without the help of key authorities. The Steganography is the art of hiding message in an image 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.

III. 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 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.

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our mainmotivation is to satisfy the strong hiding property whilekeeping the computation and communication overhead toa 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.

IV. 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 data block size and the time taken for processing the data.Different load have been used to determine the processing power and performance

V. 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 then only the information is passed. We demonstrate how to apply the proposed mechanism to high sensitive and relevant data sharing with secure and low time consuming.

.

REFERENCES

[1] Junbeom Hur 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 Loukas lazos "Packet-Hiding Methods For Preventing Selective Jamming Attacks" IEEE Transactions on Dependable and Secure Computing,vol. 9, no. 1, year 2012

[7] Umoh Bassey Offiong, M. B. Mukesh krishnan "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