Hybrid Approach for Secure Data Communication for Decentralized Disruption-Tolerant Military Networks

Mahesh Krishnan[1] Revathy M.S[2] Sonymol K.M[3] Tainu Raju[4] Prof. Sumy Joseph[5]
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]Amal Jyothi College of Engineering Kanjirapally, Kerala, India

Abstract— The information and communication technology of the present world has reached unimaginable progress breaking almost all the boundaries of imagination once perceived by the ancient man. Cryptography thus becomes an important area which provides the security of these pieces of information. The term Symmetric Cryptography employs the same key at the both ends of a message communication i.e. for both encryption and decryption. With the recent chains of calamitous events and enemy attacks, the thought of providing and supplying strong and almost never failing Disruption Tolerant Networks had been a major concern in most technocratic minds and information industries all over. The military networks share the same concern. Although a lot of encryption standards such as the DES, RSA and so on exist, none prove to be a widely accepted promising cryptographic solution like the Cipher text-policy attribute-based encryption (CP-ABE) to the access control issues. The proposed approach uses a novel method integrating the CP-ABE scheme along with fingerprint authenticated key distribution, thus the title "Hybrid Approach in Secure Data Communication.

Key words: Cryptography, Key Distribution Fingerprint, Disruption-Tolerant Network (DTN), Cipher text-policy attribute-based encryption (CP-ABE), Secure Data Communication

I. INTRODUCTION

The recent chains of various mishaps that strike a fatal blow to the numerous fields of communication networks all around the world, the necessity and demand for a more secure network that almost never fails, calls for the implementation and development of stronger Disruption Tolerant Networks throughout the world. Same is the case with the military networks. Often times, the connectivity of the wireless devices carried by the soldiers out into the field are tested through various environmental factors, jamming processes and mobility especially when they are put to operate in hostile environments. Basically when there exists no two party communication points between the sender-receiver pair, the message send from the source node may have to wait in some sort of intermediate nodes for a significant amount of time till a secure connection line or channel is efficiently established. Sir Roy [3] and Sir Chuah [4] had introduced the idea of storage nodes and system in the disruption-tolerant networks which allows data to be stored and/or replicated in such a way that only the mobile nodes are given the access to the relevant pieces of information in an efficient and sustainable manner.

In the subsidiary cases, it is often advocated to grant differential services for the accesses by way of defining the data access policies over the numerous user attributes and/or the roles available that are under the management of the key authorities that are previously defined upon. Thus the mentioned concept of the attribute – based encryption (ABE) thus evolves out into a promising approach which aims to fulfil the requirements and functionalities of the secure communication links in various channels especially the disruption tolerant networks (DTNs). When it comes to the cipher text-policy attribute-based encryption (CP-ABE), they provide a more encouraged scalable methodology of securing the data by encrypting it in such a way that the encryptor can basically define the set of attributes that the user at the receiving end should possess in order to decrypt the ciphertext where by enabling various pieces of the encrypted data as per the mentioned policy of security [5]. However, the process of incorporating the above mentioned technology in a disruption-tolerant network poses a variety of privacy issues and security challenges.

When viewed from a crypto graphical aspect the entire process can be broadly categorised into two: Symmetric Cryptography and Asymmetric Cryptography. A basic communication process is one where a sender (S) uses an algorithm (specifically known as the encryption algorithm, E) to encrypt the message (M) using a key (K) and sends the ciphertext to the receiver (R) who in turn employs a decryption algorithm (D) along with the key K to decrypt the ciphertext to retrieve the original message. Here the categorisation is based upon the type and nature of the key used in both scenarios. In the symmetric cryptography both the parties i.e. the sender and receiver uses the same key K whereas in Asymmetric Cryptography the keys used at the source end and the destination end are different. It involves two different keys, the public key for encryption and the private key for decryption. Thus the symmetric cryptography becomes a more targeted system on an average due to the fact that it employs a single and same key on both the ends.

Thus in the Symmetric Cryptography the process of distributing the keys to both the parties involved in the communication, thus becomes a challenge. They if for the purpose of communication, must share the same key and this same key must be secured and prevented from unauthorized access and modification by others. The key sharing process is trivially done in three major ways: A) The sender selects a key which is then physically delivered to the receiver. B) Both the sender and receiver have a shared common key which is employed in the past and present and so anyone of them can implement a new key and share it in encrypted form along with the previous key. C) Both the sender and the receiver are connected to another third party say Z which can select a key and deliver it to both the parties in an encrypted form.

The process of ensuring the safety and security can be achieved in a novel way by the implementation of biometrics and its related security measures in the Key Distribution Mechanism (KDM) of the above stated process. The process becomes unique and particular because like the nose prints of the cat, the fingerprints of each individual in

the whole world is unique. Normally implementation using biometrics involve the applications of biometric mediums such as fingerprint [2], face [8], retina, voice [7], iris [9] and so on. Further there is also the combinations of two or more of these characteristics in the current streams of technology. But in this case too certain problems and challenges lurk deep down. One of the major concern among them is the proper protection of the privacy of the biometric data used. It becomes significant because once the biometric identity of a user gets revealed in an environment, it results in proving the biometric data useless forever. But to minimise or better to nullify the effect, we have introduced the concept of generation of cancellable template of the biometric data in our approach provides both security and the functionality of revocability to the biometric data generated.

II. LITERATURE SURVEY

A. The Ciphertext Policy based Encryption Scheme

An attribute based encryption cryptosystem is designed with the view of enabling a more fine-grained access control of the data which is encrypted. This scheme allows the sender to attach various attributes or polices to the data or message that is encrypted so that the receiver who is allowed compatible policies or the similar attributes can access and decrypt the ciphertext. When stated formally, the attributes can be viewed in a way as Boolean variables that have arbitrary labels, and where the polices are expressed as conjunctions and disjunctions pertaining to the attribute variables. These are in fact concluded as the generalized form of the Identity Based Encryption (IBE) systems. One major difference between the two is that in the former uses only a single attribute which the identity of the receiver is often whereas the latter can use multiple attributes simultaneously. In a Ciphertext-Policy based Attribute Based Encryption (CP-ABE) system, the sender encrypts the message or data specifying a particular access policy especially in terms of access structure over the various array of ciphertext, which in turn states the way, kind or genre of the receivers who will be able to decrypt the ciphertext. The Users at the receiving end are supposed to possess sets of attribute keys from the attribute authority. Thus the receiver can decrypt the ciphertext or the encrypted data If his attribute sets satisfies the access policy which is associated with the ciphertext or the data.

B. Template Generation based on the Fingerprint

In order to accomplish the extraction of the Biometric features (B_f) from the Biometric Traits (B_t), a feature extraction algorithm (E_A) is employed. This results in the generation of a Biometric template (B_{temp}) incorporating the above ones. (i.e., $B_{temp} = E_A(B_t)$) which is used in the system of biometrics. One of the major problems of directly using this template generated is that the chances that the biometric identity of the user getting revealed in the environment resulting in a security threat is considerably high. To prevent this, we transform the original template generated into a cancellable form. In other words, we introduce a novel system of generating a 'cancellable template 'from the generated template wherein the cancellable template (T), $T = f(B_{temp})$ which uses a one-way transformation function denoted by 'f '. In order to generate multiple copies of cancellable templates from a so called single biometric trait, there are two distinct methods, (1) applying multiple functions to the biometric template (2) applying a single function to the biometric but with parameters that contain multiple transformations.

In the initial method, the number of transformation functions required is directly proportional to the number of the cancellable templates. But for the second method one function along with a number of parameters result in the generation of the cancellable templates. Thus when the need for a new template arises, the parameter is just changed which in turn results in the generation of a new template. This way, the traits of the biometry that're irrevocable can thus provide biometric data that're revocable for multiple applications without raising any concern or challenge to privacy and security. Figure 2 depicts the generation of the cancellable template with a single function and with multiple parameters of transformation.

C. Key Generation based on Biometric Properties

This is similar to most of the key generation algorithms available and employed. Here the key generation is produced on the basis of the biometric template which results in producing the cryptographic key. It generally houses a hash function which is used to generate the corresponding binary string from the biometric template. The binary string thus generated is unique, of fixed length and stable in nature. The unique key is obtained from the personal biometric using inter-person variability. This in turn becomes yet another major challenge in these systems.

The cryptographic key based on the fingerprint from the minutiae points of the user which is generally termed as the fingerprint data. The features are basically extracted from the image and the specific points are used to derive the stable key for the applications. These points are interchanged to make the revocable form which is then subjected to a novel key generation algorithm which generates the revocable key contrary to the irrevocable fingerprint biometrics.

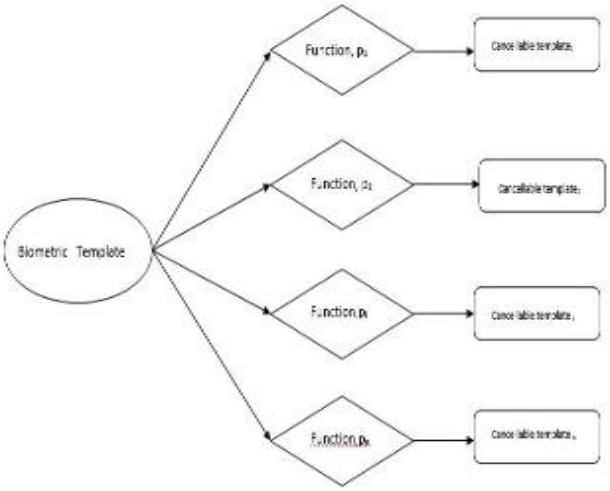

Fig. 2: Cancellable Template Generation with a Single function and with multiple Transformation Parameters

III. PROPOSED SYSTEM

In this section, we propose a multi authority Ciphertext-Policy based Attribute Based Encryption (CP-ABE) system that aims in secure data retrieval in decentralized DTNs.

Each of the local authority are given power to issue personalized forms of partial attribute key components to a user group (basically to the members of the battalion) by performing what is known as a secure Two Party Communication Protocol or basically known as the 2PC protocol that is associated with a central authority along with the application of biometric encryption. Thus the proposed system induces a 'Hybrid' yet a novel way of approach securing the data communication in these networks.

Since its inception and coining of the term by Bethencourt et al. [5], the CP-ABE scheme proposed by him has undergone a tremendous series of changes and almost a dozen variants of the initial Ciphertext-Policy based Attribute Based Encryption (CP-ABE) schemes have been introduced into the field of cryptography and communication systems. Quoting this eminent personality, what we have humbly tried upon is to bring out yet another variation of the Ciphertext-Policy based Attribute Based Encryption (CP-ABE) system which is partially based on (but in fact not limited to) Mr. Bethencourt et al.'s [5] and sir Junbeom Hur's [1] and sir Kyungtae Kang's [1] construction in a way to enhance the existing features and expressiveness of the various policies such as the access control policy and the key distribution centre or the process of key distribution in general instead of construction a whole new Ciphertext-Policy based Attribute Based Encryption (CP-ABE) scheme from the dirt.

The proposed system also contains biometric element added onto it. The biometric referred here is the fingerprints. For the purpose of introducing the fingerprint of the sender commander into the communication system, we enrol the fingerprint of the sender (the commander) into the database of Key Distribution Centre (KDC db). The whole process of enrolment of the sender is depicted in figure 2.1. When the fingerprint of the sender is scanned, the features actually mapped are the minutiae points. Once the minutiae points are extracted, then the biometric template is generated which in turn is applied some transformation function (possibly using the Cartesian transformation, as discussed in [6]) to obtain the revocable cancellable template. This is used to increase the security of the biometric in the electronic system, protecting the unique identity of the user if (in any case) it gets compromised. Once this is generated, the template is then added onto the KDC database along with a unique User identification number (Uid)corresponding to each of the entries.

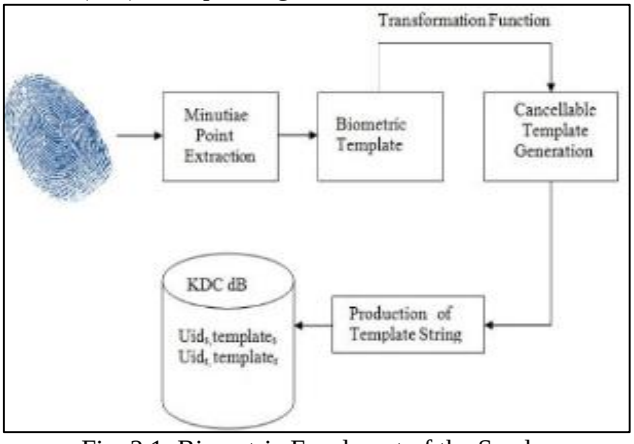

Fig. 2.1: Biometric Enrolment of the Sender

The sender for sending out the data encrypts it using the above Template form and the Two Party Communication key (2PC Key) generated by the Key Authority. The encrypted data is then sent to the storage node. The entire transactions of the process can be seen in figure 2.2.

By using the template form basically includes generating a permanent key which the KDC does when the party requests, using its assigned Uid. This happens on both the ends of the string. The generation of the 2PC key can be done by one key authority or by more local key authorities who then sent their individual key parts to central key authority. For instance, if the 2PC key is supposed to of 16 character long, it's possible to setup 4 local key authorities who can in turn create 4 individual portions of the final key using different sets of seeds consequently increasing spectrum of possible combinations exponentially, The user or the soldiers whose attribute sets and access policies are satisfied, can request a permanent key version of the template from the KDC using the Uid provided. Together with this and the 2PC key, they can decrypt the information.

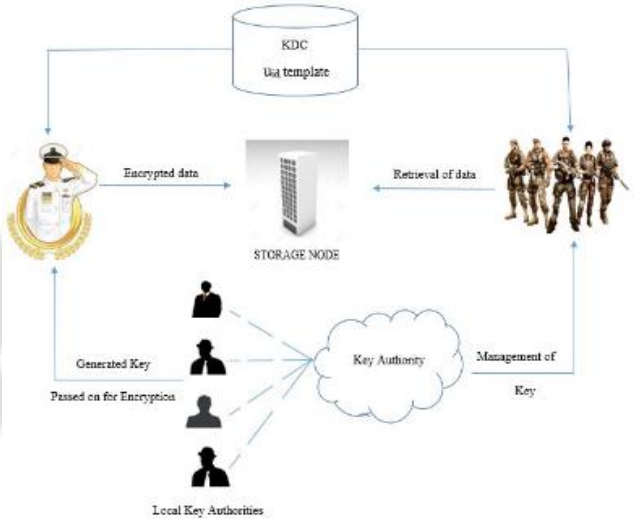

Fig. 2.2: Proposed Architecture of the System

IV. CONCLUSION

We are currently going through a global scenario where in the question of military supremacy and sustainable efficiency of these are put into vigorous tests, that too, in ways unimaginable. It is yet another naked but blunt truth that the nation which has the strongest armed force gets to have the last word even in the global affairs. The disruption tolerant network technologies thus become one of the interested areas of military research as such applications are indeed capable of wireless communication and also tapping to the confidential feeds reliably, by exploiting the loopholes in the external storage nodes. The Ciphertext-Policy based Attribute Based Encryption (CP-ABE) systems, thus can be proposed as promising cryptographic solution to various issues of secure data retrieval and access control forms with an added advantage of scalability in their structure. In this paper we proposed a hybrid, efficient approach for secure and reliable communication of sensitive data two and fro, employing the Ciphertext-Policy based Attribute Based Encryption (CP-ABE) scheme along with the Fingerprint managed Key Distribution Centre for the decentralized disruption tolerant military networks. The proposed system

is thus expected to widen the horizon of researches for more sophisticated implementations and derivations of the technology, thus revolutionising the entire idea.

REFERENCES

[1] Junbeom Hur and K. Kyang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks," IEEE/ACM 2014
[2] Subhas Barman and Samiran Chattopadhyay and Debasis Samanta, "An Approach to Cryptographic Key Distribution Through Fingerprint Based Key Distribution Center," IEEE 2014
[3] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[4] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.
[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attribute Based Encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancellable Fingerprint Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561-572, April 2007.
[7] Monrose, F., Reiter, M. K., Li, Q., and Wetzel, S. "Cryptographic key generation from voice." In Proceedings of IEEE Symposium on Security and Privacy, 2001, pp. 202-213
[8] Chen, B., Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," In Proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, vol., no., pp.394-401, 2007.
[9] Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, 2006.

