A SURVEY ON ENCRYPTION ALGORITHMS FOR DATA SECURITY

A.Rekha[1], P.Anitha[2], A.S.Subaira[3], C.Vinothini[4]

[1]PG scholar, Department of CSE, Dr.N.G.P Institute of Technology, Tamil Nadu, India
[2]Assistant Professor, Department of CSE, Dr.N.G.P Institute of Technology, Tamil Nadu, India
[3]Assistant Professor, Department of CSE, Mahendra College of Engineering, Tamil Nadu, India
[4]Assistant Professor, Department of CSE, Dr.N.G.P Institute of Technology, Tamil Nadu, India

Abstract

In current world the security is more important in all fields. The data that is transferred between any must be retrieved securely. For this secure data retrieval we use cryptographic solutions. Disruption Tolerant Network (DTN) technologies have become successful solutions that permit wireless devices to speak with one another and access the guidance dependably by exploiting auxiliary storage nodes. The cryptographic solutions used for the retrieval of data are encryption algorithms. In this paper we discussed several algorithms used for the secure data retrieval in all fields.

Keywords: *Security, Cryptography, DTN and Encryption*

--***--

1. INTRODUCTION

Network security prevents the data in a network from unauthorized access. It involves the authorization of access to information throughout a network and it is measured by network administrator. The need for security is to protect the information as well as provide authentication and access control for resources, guarantee availability of resources. A mobile ad hoc network (MANET) is a continuous arrangement of large network of moving devices that are not connected wires. The MANET characteristics are dynamical topology like mobile devices join/leave the network unexpectedly; they will conjointly move freely, every node conjointly is router; facilitate to relay packets received from neighbors. An associate degree rising application area for MANETs is Wireless Sensor Network (WSN). The security requirements in MANETs are accessibility, authorization and key management, data privacy, data purity, non disapproval. The challenges in knowledge networking are sensors, intermittent property, long-delay links, need revisiting ancient assumptions. The challenged networks area unit containing options or needs a networking design designer would notice shocking or tough to reason, or in operation atmosphere makes communications tough. Examples: mobile, power-limited, far-away nodes human activity over poorly or intermittently available links. Challenging Environments are random or predictable node qualities like Military/tactical networks, Mobile routers with disconnection, daily schedule for a automobile moving by a small town, stages of whole separation, massive delays and low information measure, massive delays and high information measure. Disruption Tolerant Networking (DTN) is new space of analysis and standards with several application situations with distinctive properties. DTN routers type associate overlay network like solely nodes are selected that have persistent storage is participated. Topology of this routing might be a time-varying impress like links come back and go, use any/all links which will presumably scheduled, predicted, or forced Links, could also be target aspect, may acquire from report to judge the plan. Fragmented messages supported dynamics are proactive fragmentation: optimization of contact volume, reactive fragmentation: resume wherever you unsuccessful. In a network communication between two hosts should be encrypted to enhance security. There are different types of encryption algorithms used for transferring the data securely.

2. ENCRYPTION TECHNIQUES

Encryption is that the method of coding messages in a way that solely licensed parties will read it. Encoding denies the message content to the fighter. The original messages are considered as a plaintext. The plaintexts are encrypted to a cipher text. The encryption is done by encryption algorithm. The cipher text is decrypted to get the plaintext. The encryption algorithm generates key for encrypting the plaintext. The receiver who has the key is called authorized one, so they can able to decrypt the cipher text. Unauthorized person who does not have the key cannot able to decrypt the text. Encryption is used for data protecting while transferring.

2.1 Encryption Types

2.1.1 Symmetric Key Encryption

For both encryption and decryption same keys are used in symmetric key encryption. It is secure if both keys are the same. The message can be decrypted if the unauthorized person knows the key. The problem here is management of keys, transforming the keys securely not the messages. Keys are generated before the message because it is smaller than the messages.

2.1.2 Asymmetric Key Encryption

For both encryption and decryption different keys are used. Hence the key management problem is overcome. Both the keys are sufficient for encrypting and decrypting the message. A pair of key is used; one key for encrypting and other is for decrypting the message. Private/Public key is used encrypting/decrypting message.

3. ASYMMETRIC KEY ENCRYPTION

It is also known as public key encryption algorithm. The use of public key cryptography is public key encryption. Based on the public key encryption there are many algorithms for transferring the message securely. The security in public key encryption is confidentiality, the sender encrypts the message using receiver public key and it is decrypted only by the receiver paired private key.

3.1 Identity Based Encryption Algorithm

Shamir [13] and Boneh et al. [11] introduces Identity-Based Encryption (IBE) with an efficient determinable bilinear map. Halevi et al. [12] put forward IBE in a random oracle representation. The efficiency is increased by the two schemes in outside random oracles that were proposed by Boyen et al. [10]. Sahai et al. [4] introduces different type of Identity-Based Encryption (IBE) called Fuzzy Identity-Based Encryption. A set of descriptive attributes is viewed as an identity in Fuzzy IBE. It is used for application like Biometric identities in IBE and attribute-based encryption. They proposed error tolerance between the identities of keys that are used for encryption. In Fuzzy-IBE there are few problems. If attributes come from multiple authorities, the Fuzzy-IBE is possible or not.

3.2 Attribute-Based Encryption

Sahai et al. [4] proposed Attribute-Based Encryption (ABE) in Fuzzy IBE. The secret key is based on a set of attributes. While decryption the set of attributes must match cipher text attributes.ABE has two types: Key-Policy ABE (KP-ABE), Cipher text-Policy ABE (CP-ABE). In Key-Policy ABE [5], the cipher text is encrypted with the attribute set. For decrypting, the policy is chosen by the key authorities. **Fig - 1**: represents the schematic representation of Attribute-Based Encryption [14]. Based on the attributes the signature of information takes place.

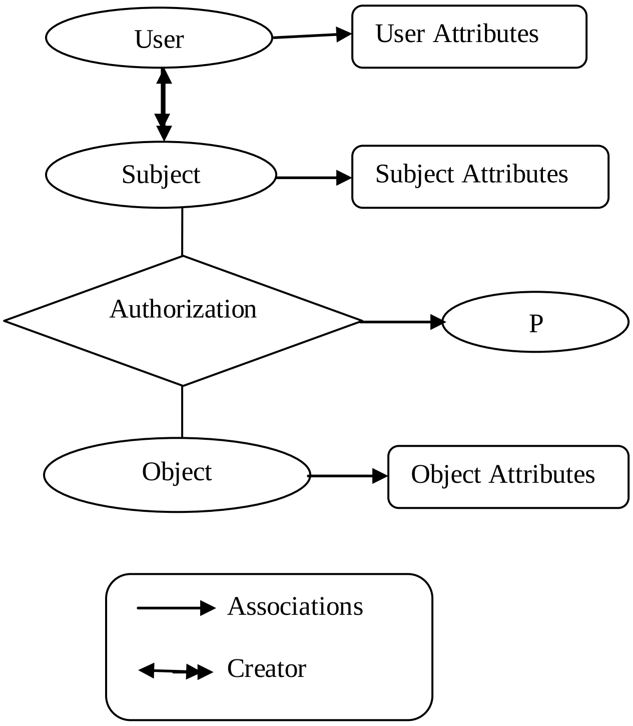

Fig -1: Overview of ABE based access control model

3.2.1 Mediated Cipher Text-Policy Attribute-Based Encryption

Ibraimi et al. [2] proposed mediated Cipher text-Policy Attribute-Based Encryption (mCP-ABE) based on mediated cryptography. It is an extension of CP-ABE with rapid attribute revocation. The cipher text is decrypted by the user only if the access policy is satisfied by the attribute set of secret key. Cipher text is related with an access policy. The user secret key is related with a set of attributes .Once attribute is revoked, it cannot able to decrypt by user. The drawback is attribute revocation must be self- addressed that is before expiry date, the user cannot able to revoke an attribute.

3.2.2 Multi Authority Attribute-Based Encryption

Chase [9] proposed Multi authority Attribute-Based Encryption in a fine grained access control ABE. They proposed schemes that permit polynomial number of individual authorities and accepts the random number of dishonest authorities. Later Lewko et al. [3] present this algorithm in new version. The authority can be anyone and it doesn't require any coordination between authorities. It doesn't need a central authority. The algorithm is scalable by preventing the occurrence incurred by depending on central authority. In addition to scalable, efficiency and security is also enhanced.

3.2.3 Attribute-Based Encryption with Non-Monotonic Access Structures

Attribute-Based Encryption with Non-Monotonic Access Structures was introduced by Waters et al. [7]. In an attribute the private key of users can be articulated by any access rule. Earlier ABE algorithms uses only monotonic access structure, this limitation is overcome by this algorithm. While conserving collusion resistance structure they encounter challenges because of the negation method.

3.2.4 Bounded Cipher Text-Policy Attribute Based Encryption

Goyal et al. [8] proposed Bounded Cipher text-Policy Attribute Based Encryption, having a security proof based on a number theoretic assumption. It encourages the access policy signified by bounded size access construction along with the nodes having threshold gates. With certain variations it supports non-monotone access structure.

3.2.5 Cipher Text-Policy Attribute Based Encryption

Cipher text-Policy Attribute Based Encryption (CP-ABE) was introduced by Bethencourt et al. [6] .CP-ABE is encrypted data for complex access control in a system. The set of attributes provide the private key for users. The policies are specified by the party who is encrypting data over the attributes that specifies which user can able to decrypt. This algorithm keeps the encrypted data as confidential and secure opposed to collusion resistance. This algorithm allows any monotone access structure, single authority and periodic attribute revocation. Key escrow is not addressed. To overcome the limitations of previous CP-ABE are overcome and it is intended by Hur et al. [1].The attribute revocation, key escrow and attributes coordination that are issued by different authorities are solved using this algorithm. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed where key authorities may be compromised. For each attribute group the fine-grained key revocation should be done. The components of a partial personalized and attribute key to a user issued by the local authority, by performing secure 2PC protocol with the central authority. The user attribute key can be updated individually and immediately. Thus, the scalability and security can be enhanced.

4. CONCLUSION

In this paper we discussed about cryptography in network security and various encryption algorithms used in cryptography to improve the data secrecy. The different encryption techniques determine the importance of encryption that it allows us to confidently protect data so that it cannot be accessed by any other person. These encryption methods are used to safeguard the business confidences, to safeguard the government top secret information and to safeguard plenty of people's private information. We mainly focused on public key encryption algorithms to protect the data across network. In public key encryption there is no necessary for sharing the keys. Diffie–Hellman key exchange method is used in many of these encryption algorithms. This key exchange makes it desirable to securely transfer the data more protectable over an unsafe network. Diffie-Hellman key exchange method is a way in which people may generate combined confidential information that cannot be estimated by snooper. These various encryption algorithms lead to the importance of information confidentiality in all fields.

REFERENCES

[1]. J. Hur and K. Kang,"Secure data retrieval for decentralized disruption-tolerant military networks", in Proc. IEEE/ACM Transactions on Networking,2014.

[2]. 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.

[3]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptology ePrint Archive: Rep. 2010/351, 2010.

[4]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.Eurocrypt, 2005, pp. 457–473.

[5]. 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.

[6]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.

[7]. 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.

[8]. V.Goyal, A. Jain,O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

[9]. M. Chase, "Multi-authority attribute based encryption," in Proc. TCC,2007, LNCS 4329, pp. 515–534.

[10]. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[11]. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[12]. Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

[13]. Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[14]. B. Balamurugan and P. Venkata Krishna. Extensive Survey on Usage of Attribute Based Encryption in Cloud. In Proceedings of Journal Of Emerging Technologies In Web Intelligence, VOL. 6, NO. 3, 2014, pp.263-272