IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

# Review on Different Encryption Models for Data Security

**Mr. K. S. Satpute[1], Mr. M. J. Pande[2]**

Asst. Prof., Dept. of CSE, DMIETR, Sawangi (M), India[1]

Asst. Prof., Dept. of CSE, AVBIT, Pawanar, India[2]

**Abstract:** In day to day life, the digital communication is very useful and growing faster as a need of human resources for communication. The growth of the internet and communication networks is also a developing necessity for easy and secure user-to-user message transfer. As sharing of information is an easier task due to the communication network need to concentrate on the security of information. The different model is available to provide the security on a various parameter, this paper focuses on the Conventional Encryption i.e. Public Key-Private Key Encryption, Identity-Based Encryption (IBE), Attribute Base Encryption (ABE) that provide the security.

**Keyword:** Encryption, Public Key, IBE, ABE.

## I. INTRODUCTION

Conventional encryption ciphers rely on a single key for both encryption and decryption. Modern world will use a private key for encryption and a different public key for decryption. These two keys are mathematically related in a fashion that allows them to encrypt/decrypt the same data successfully. Identity-based encryption (IBE) is a form of public-key cryptography proposed by Adi Shamir in 1984 in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages.
Attribute-based encryption (ABE), introduced by Sahai and Waters (2005), offers an expressive way to define asymmetric-key encryption schemes for policy enforcement based on attributes. User secret key and cipher text are related with sets of attributes. There are two flavours of ABE defined, i.e. cipher text-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE).

## II. DIFFERENT MODEL

### 1. Conventional Cryptosystems

In the conventional encryption process. The original “plaintext” is converted into apparently random nonsense, called “cipher text”. The encryption process consists of an algorithm and a key. The plaintext and encryption key is independent. The algorithm will produce output depending on the specific key being used at the time. Changing the key changes the output of the algorithm, the cipher text.Once the Plaintext converted into cipher text, it is ready totransmit. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security of conventional encryption depends on several factors:

a. The Encryption Algorithm. It must be powerful enough that it is impractical to decrypt a message on the basis of the "cipher text" alone.

b. Secrecy key- It was shown that the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text.**Y=Ek (X)**
The intended receiver, in possession of the key is able to invert the transformation

**X=Dk (Y)**

### 2. Identity-based encryption (IBE)

Public-key cryptography offers very strong protection for electronic communications. Much of its strength comes from the use of paired keys, which are separate but mathematically related codes that encrypt and decrypt a message; one key is public and one is known only to the recipient. The recipient has to be prepared with both public and private keys, and the sender has to know or be able to find the recipient's public key.
Identity-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Key Distribution Centre (KDC), generates the corresponding private keys. To operate, the KDC first publishes a master public key, and retains the corresponding master private key i.e. master key. Given the master public key, any party can compute a public key corresponding to the identity by combining the master public

key with the identity value. To get a corresponding private key, the userapproved to use the identity ID contacts the KDC, which uses the master private key to generate the private key for identity ID.

**An IBE system involves a set of four algorithms.**
**Setup:** A Key Distribution Centre (KDC) generate global system parameters and a master-key which the KDC keep safe. The whole security of the system relies on the safe keeping of this master-key
**Extract:** The KDC runs an extract algorithm inputting the user's identity parameters and using the master-key from the setup. The output is the user's private-key associated with the user's identity. It's important that the private-key is transported to the user in a safe manner and th at the KDC has made a full examination of the user credentials before issuing a key corresponding to those credentials.
**Encrypt:** A probabilistic algorithm. Any user encrypts using the global system parameters and public key. The output is the cipher text.
**Decrypt:** This process takes the cipher text from the encrypt function, global system parameters and the private key issued by the KDC. The output is the corresponding plaintext.

**3) Attribute-based encryption (ABE)**
In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based encryption changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (Key-policy ABE - KP-ABE) or policies defined over a set of attributes (Cipher text-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

**a) Cipher text-Policy ABE**
In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. Policies may be defined over attributes using conjunctions, disjunctions and (k,n)-threshold gates, i.e., k out of nattributes have to be present. For example, let us assume that the universe of attributes is defined to be {A, B, C, D} and user 1 receives a key to attributes {A,B} and user 2 to attribute {D}. If a cipher text is encrypted with respect to the policy (A∧C) ∨D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.
CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice features is, that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

**b) Key-Policy ABE**
KP-ABE is the dual to CP-ABE in the sense that an access policy is encoded into the users secret key, e.g., (A∧C)∨D, and a cipher text is computed with respect to a set of attributes, e.g., {A,B}. In this example the user would not be able to decrypt the cipher text but would for instance be able to decrypt a cipher text with respect to {A, C}.
An important property which has to be achieved by both, CP- and KP-ABE is called collusion resistance. This basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a cipher text that neither of them could decrypt on their own.

## III. CONCLUSION

In the digital communication era data security is most important, the various security algorithm and model is available to secure the information. In this review paper try to focus on three modelConventional Encryption, Identity Based Encryption (IBE), and Attribute Base Encryption (ABE) that will help us to provide a way to protect the data or information

## REFERENCES

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing, extended abstract. In Crypto '2001, volume 2139 of Lecture Notes in Computer Science, pages 213-229. Springer-Verlag, 2001
[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM Journal of Computing, 32(3):586—615, 2003.
[3] http://www.computerworld.com/article/2551479/security/identity-based-encryption.html
[4] http://doras.dcu.ie/17368/1/neil_costigan_20120703114211 .pdf
[5] https://discovery.csc.ncsu.edu/Courses/csc774-S08/reading-assignments/shamir84.pdf