

# Encryption techniques & access control models for data security: A survey

Rashmi Dixit <sup>1\*</sup>, K. Ravindranath <sup>2</sup>

<sup>1</sup> Research Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502

<sup>2</sup> Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India 522502

\*Corresponding author E-mail: rashmirajivk@gmail.com

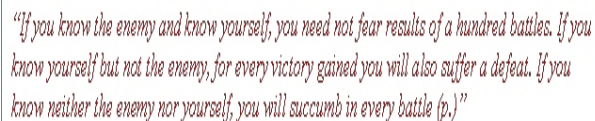
## Abstract

In the process of sending information from sender to receiver, an unauthorized user may work in an active way (update it) or passive way (read or delay in sending). There must be some techniques which assures receiver that whatever information received from authorized user as well as must be same as sent from sender side, in addition to this receiver never make Denial of service. Nowadays sharing of information or resources is a very common thing from single user to the network to the cloud. When information is moving from one node to another node, security is a big challenge. When information is stored on the user's computer, it is under control but when it is in movement user lose control over it. In the world of security, to convert information from one form to another form, Encryption is used, so that only authorized party will able to read. Encryption is a technique for any security-conscious organization. In this paper, we present basic access control models along with encryption techniques.

**Keywords:** Encryption, Access controls Model, Confidentiality, Integrity, and Availability.

## 1. Introduction

Today everyone starting from single person to a big organisation has their own information system and they want to keep their information secure. Any attack on information leads to serious damage in terms of short-term as well as long-term.



*"If you know the enemy and know yourself, you need not fear results of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle (p.)"*

Fig 1: Chinese quote

As stated in fig 1, this 2500-year-old quotes points out how information, as well as information stealer (attacker) both, are important for a particular user. Before keeping information secure, we must aware of inherent features of attack to prevent attack.

An audit conducted by one of the famous Lab demonstrated that, in most cases, whatever comes to know attack is only the tip of the iceberg. 74% reports mention that there are other not known security attacks which get coincides with such known attacks. This survey gives seriousness about system security. Common mechanism for providing security and to protect users data are encryption, authentication or authorization.

Encryption is a method which encodes intelligent plaintext into the scrambled message so that only intended receiver is able to

read it. To encrypt message two things are required, algorithm and key. Depending upon the number of keys used there are two types of encryption first one is Symmetric (which is known as Private key encryption) in which the same key is used at both sender and receiver side and the second one is Asymmetric (known as Public key encryption) in which two keys, different ,at sender and receiver side are used. It provides confidentiality to information among authorised and unauthorised user.

Access control is one of the techniques for security for providing integrity and confidentiality. Its main task is to regulate the sharing of resources or information. Access control denotes whether a particular user has rights to perform particular operation on particular data. Access control policies define the users' permission in order to provide security. These policies are defined according to an access control model. It prevents unauthorised sharing of resources or information. It also secures data against internal attacks and disclosure, leakage of information to cyber-terrorist.

## 2. Access control and access control models

Mostly Access control is user identification to do a specific job, provide authentication, then provide that person the right to access data This is just like granting an individual permission to log in to network using name and password, allowing then to use resources after confirming whether they have permit to do particular job. So, how to provide permission to a particular user to perform their task? Here access control is used.

Access control term was first used with formal notions of, subject, objects and access control matrix. Simple matrix representation in

which each entry [i, j] represents operation granted to particular subject i on object j.

**Table 1:** A sample access control matrix

	Student Data	Office Data	Administrative data
Alice	W,R	R	
Bob		R	R
Charley	R	W,R	W,R

As shown in above Table 1, for each user (object) grant permission are recorded in the matrix.

Access control models have four Types “Mandatory Access Control” (MAC), “Role Based Access Control (RBAC)”, “Discretionary Access Control (DAC)”, and “Rule Based Access Control (RBAC or RB-RBAC)”.

#### 1. Discretionary Access Control or DAC

When using DAC method, the holder has a right to provide access to the resource. So decisions about users are made precisely. To accomplish this, Access Control Lists (ACL) is used. ACL enlist rights or permission for the particular user. The permissions identify the activities particular user can perform with particular data.

#### 2. Mandatory Access Control or MAC

MAC is a rigid fixed, most effective in maintaining confidentiality access control method. This model is suitable for the hierarchical organization as security levels are related to information flow in which end users are not able to settle its own permission as information is the property of the organization. MAC control access according to subject clearance and objects classification which is divided in level according to security. Only administrators have rights to assign objects security level, not data owner. Only the data owner has the privilege to take the decision about matching of authorisation requirement to see the particular data. All users can read data from the lower level and write to the higher classification. Access is restricted to object depending upon the label.

#### 3. Role Based Access Control

This is a combination of MAC and DAC. The roles are assigned to each subject. Permission is associated with roles not to direct user. The role can be a coder, group manager, or administrator. A user represents some role which permits them to use particular resources. Accessibility of Data is determined by roles not users. Roles are hierarchical not a flat collection of permission.

#### 4. Rule Based Access Control

Rule-based access control simply defines the guidelines to allow or to reject permission to use particular resource. It dynamically assigns roles to the user. If the guideline allows, then only particular will be able to use particular resource. The best example of usage is routers with their access control lists. Access control list maintains the record if IP address which have permission to pass through router. Only single rule is defined in this case. In this method, there are no accounts, membership or security labels.

## 3. Encryption Methods

### 1. Attribute Based Encryption (ABE):

The two major goals of ABE are to provide access control and security. ABE uses public-key with one to many encryptions. Users using this encryption method encrypt and decrypt data based on their user attributes. The characteristics of ABE schemes are as follows:

### 1.1 Data confidentiality

Data confidentiality is a set of rules that limits access or places restrictions on specific types of information and allows only specific, authorized users to access resources. In cloud, the data is encrypted by the owner of the data and unauthorized parties. No party, including those using the cloud, can know the information of the encrypted data. Therefore, data confidentiality is maintained.

### 1.2. Secured access control

Secured Access Control is the mechanism by which a cloud system grants authority to an individual to access some data, or perform some action. While using the resources in cloud, users are granted with different access rights to access data to provide security.

### 1.3. Scalability

Scalability is defined as the capability of the system to handle the user load, number of transactions, the data volume etc. When there is increase in the number of authorized users, a scalable system can work efficiently. The increased number of authorized users cannot hamper the performance of the system.

### 1.4. User accountability

If the authorized user is not honest, he would share his private key with the other unauthorized users. This may cause serious problems, and the illegal key would be shared among unauthorized users leading to security problems.

### 1.5. User revocation

If the user quits the system, this scheme can revoke the user access from the system directly. Such a user whose access was revoked cannot access any stored data.

Two types of ABE, first one is key-policy ABE schemes (KP-ABE), in which cipher text is commented with set of attributes. Trusted third party generates private key for user along with guideline to describe which sort of ciphertext can be decoded. Second one is Cipher text policy ABE (CP-ABE) operates first, by attaching attribute to private keys, and at the same time sender mention guideline which must be collaborates with receivers' attribute sets.

### 2. Role Based Access Control:

Role-based access control (RBAC) is a method to which provide contact with a system based on the role of the particular user in the organization. The technique is around roles on which privileges are defined. The ingredients of RBAC help to make user appointment simple. In the world of Information Security, access control term used to define access or permission to particular resource RBAC helps to defines complex access control policies, with less error and cost.

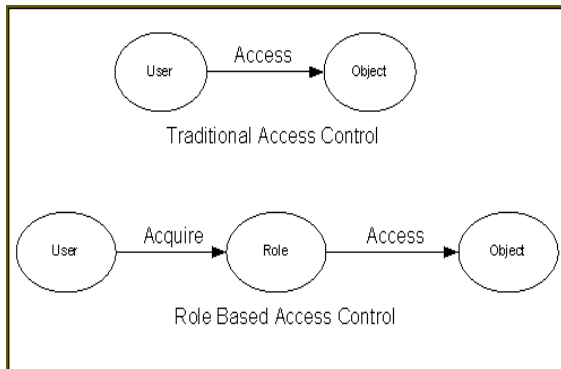


Fig. 2: Role based access control

### 3. Attribute Based Access Control:

Attribute based access control is an authorization model that provides lively, background-based rational liability access control. It is combination of attribute with transparent guideline to provide access to a particular user with specific rights .It helps to meet effective consent, time reduction for new domain market entry.

### 4. Proxy Re-Encryption Technique:

These are cryptosystems in which sender before sending converts plaintext into cipher, new entity called as proxy is introduced to re-encrypt a cipher which gets decrypted at receiver side .PRE schemes can be divided into two types that is duplex PREs and simplex PREs. In duplex PREs, the proxy can operate from sender to the receiver and also in opposite direction i.e. from receiver to sender. In contrast, the proxy in simplex PRE cannot operate on the cipher text in the receiver to sender side direction.

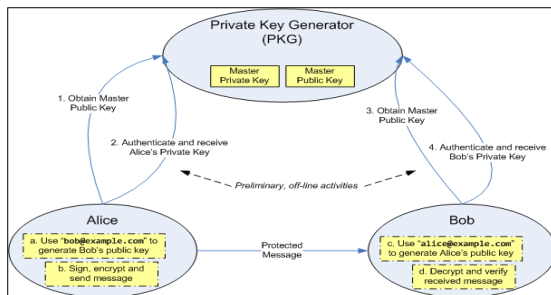


Fig 3: Identify based encryption

### 5. Identity Based Encryption:

An identity based encryption (IBE) scheme is a Asymmetric encryption where any word representing the identity of a user like email id, or IP address may be a authorized public key is a valid public key. Public key infrastructure (PKI) allows digital signature. Identity-based systems allow any entity to create a public key from a known identity.

### 6. Identity Based Proxy Re-Encryption:

This is the combination of Identity Based Encryption along with Proxy based re-encryption.

In identity based proxy re-encryption, sender encrypts the message using recipient identity as a public key. An IBCPRE scheme is having two aspects.

Proxy re-encryption took the approach of identity based re-encryption technique.

### 7. Ciphertext Policy Attribute Set Based Encryption:

In CP-ABE, user with some credential and cipher text itself carry along them guideline to decrypt. The user is able to decode cipher, if and only if its credential matches with guideline cipher text.

### 8. Hierarchical Attribute Based Encryption:

Working in a various domains like cloud computing, data mining, user store data outside its control. To keep data secure HIBE is used as the name suggests is the generation of keys in a hierarchical way. Just structure like tree, the credentials of user may inherit to higher one.

## 4. Literature review

Y.Zhang, J.Chen, R.Du [1] In this paper, they proposed a "Flexible and Efficient Access Control Scheme" (FEACS) based on Attribute-Based Encryption, which helps to setup transparent guideline for security which provide data confidentiality .They also provide detailed analysis of performance also five comparisons with other models

B.Water[2] In this paper they represented a method for accomplishing the "Ciphertext-Policy Attribute Encryption" (CPABE). With the help of this schema, any sender can write their own formula with aspect to provide solution.

B.B, V.P [3] In this paper they have given broad survey on control of attribute based encryption in cloud. Attribute based encryption that used to clarify users from collecting data .One of the main reason to use of ABE is power of key which provides stronger encoding.

V.Goyal,O.Pande,A.Sahai[4], they developed a system for sharing of encrypted data that happens in fine grain way .In this system cipher are annotate with attributes along with private keys which provide guideline for access of cipher for the decryption at the receiver side

D.R.Kuhn,E.J.Coyne,T.R.Weil[5], Role-based access control (RBAC) is a method to which provide contact with a system based on the role of the particular user in the organization. The technique is around roles on which privileges are defined .It also compares RBAC with ABE

G.Ateniese, K.Fu, M.Green[6] ,they proposed an application called atomic proxy re-encryption,

As compared to PRE ,instead of proxy, semi-trusted entity is established which converts cipher from sender before send to receiver without seeing original intelligent message

F.Wang,Z.Liu,C.Wang[7] In this paper they proposed an efficient identity-based encryption (IBE) scheme. IBE scheme is a Asymmetric encryption where any word representing the identity of a user like email id, or IP address may be a authorized public key is a valid public key. Public key infrastructure (PKI) allows digital signature. Identity-based systems allow any entity to create a public key from a known identity .Semantic rules are also used.

M.Green,G.Ateniese[8] In this paper, they discuss the problem of IB-PRE, where encryption done on the basis of identity.

G.wang,Q.Liu,J.Wu[9] they proposed method to mix HIBE with CP-ABE to provide more confidentiality when data is not under the control of user. They also make effective use of proxy re-encryption along with lazy scheme which give expressive increase in performance.

J.Liu,Z.wann,M.Gu[10] They proposed scheme that derive resilience long with attributes. It provides graded structure due to hierarchical organization. User automatically gets cancelled as expiration time is gradually increasing which is mentioned in attribute set.

Mohammed ENNAHBAOUI, Said ELHAJJI [11] presented broad survey on access models.

Juan M. Marin Perez, Gregorio Martinez Perez, Antonio F. Skarmeta Gomez [12] works on data in motion. They provide encryption to data as encryption to authorization model which store privileges for the user about that particular data

## 5. Conclusion

Access Control is the primary thing for security and is used to protect private and confidential data from attack. Basic access control understanding helps us to manage information security. Four basic models are discussed here. Apart from these four, several models have been developed to increase authenticity, integrity, confidentiality. Another way to provide security is the encryption which uses mathematical algorithm with proper key to perform operation.

Both encryption and access control are used for privacy and to prevent unauthorized users from accessing some object. That data will be in motion so copy or deletion will be possible. With ACL, you can just allow or reject access on a software level not on physical storage. Encryption is used to provide confidentiality of data but data may be access by untrusted entity. Access control is used to provide limited access to the particular entity to particular user as defined by owner. The ACL and encryption, these both things are different in their working as well as in concept but their main aim is to provide security. Encryption can provide very strong controls over data confidentiality, But it is difficult to manage when lots of user access the same data but is difficult to get right, can be computationally expensive. As lots of mathematical functions are involved it somewhat computationally complex. Encryption also not so easy when needs is different like some need data to read only while other need to write and some need for both. If complex relationship exists between user and data, access control is much more flexible and easier to implement, but it is only implemented by the code that is running on the system. In such cases access control are weaker

## Acknowledgement

This paper is made possible through the help and support of Principal, Dean (R&D Dept) Head of CSE department, Guide of KL University, Vaddeswaram, Guntur, A.P as well as family and friends'. The product of paper is not possible without them.

## References

- [1] Y.Zhang, J.Chen, R. Du. "Feacs: A flexible and Efficient access control scheme for cloud computing"2014
- [2] B.water "ciphertext –policy attribute-based encryption an expressive, efficient and provably secure realization"2011
- [3] B.B, V.P "extensive survey on usage of attribute based encryption in cloud"2014
- [4] V.Goyal, O.Pande, A.Sahai, B. Water "Attribute based encryption for fine-grained access control of encrypted data" 2016
- [5] D.R.Kuhn, E.J.Coyne, T.R.Weil "Adding Attributes to role based access control"2010
- [6] G.Ateniese, K.Fu, M.Green, S.Hohenberger "Improved proxy re-encryption schemes with application to secure distributed storage" 2006
- [7] F.Wang, Z.Liu,C.Wang" Full secure identity based encryption scheme with short public key size over lattices in the standard model"2015
- [8] M.Green,G.Ateniese "Identity-based proxy re-encryption"2007
- [9] G.Wang,Q.Liu,J.Wu "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services"2010
- [10] J.Liu,Z. Wan,M.Gu "Hierarchical attribute-set based encryption for scalable ,flexible and fine-grained access control in cloud computing"2011.
- [11] Mohammed ENNAHBAOUI Said ELHAJJI "Study of Access Control Models", Proceedings of the World Congress on

Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013, London, U.K.

- [12] Juan M. Marin Perez, Gregorio Martinez Perez, Antonio F. Skarmeta Gomez "SecRBAC: Secure data in the Clouds" IEEE Transactions on Services Computing (Volume: 10, Issue: 5, Sept.-Oct. 1 2017).
- [13] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273, August 2014.