# Implementation of Secure Production Database System by Using AES and RBAC

Pwint Wai Hlaing, San Thida
*University of Computer Studies,Yangon*
*mpwh.miemie@gmail.com*

## Abstract

*Protecting privacy and ensuring the security of very important data and operations in an organization are essential need for the detergent production organization. Access control is the important mechanism for protecting information from unauthorized user and access. And as the access control is an essential need, the security of data in database is an essential and important need too. No matter what degree of security is put in place, many conventional database security systems are bugged with holes that can be used by attackers to penetrate the database. So the sensitive data in database are still vulnerable to attack. Since both the access control and security of data are the essential need for a system, this paper describes based on the two security mechanisms: role based access control (RBAC) and advanced encryption standard (AES).The system provides the security of production system that has sensitive data e.g, the formula of each production of the product.*

## 1. Introduction

Access control can define not only who or what process may have access to a specific resource, but also the type of access that is permitted. In the case of access control, there are Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). RBACs are defined by job function and are definable with much more control. An RBAC can provide security administrator with the ability to determine who can perform what actions, in what order, and in some cases under what relational circumstances. However no matter how the access control mechanism of the system is high, the attacker can attack from the database that stored data. Although the database systems have security system, they can have leaks that attacker can use to penetrate the database. So the data in the database can still be easy to attack. So a remedy is to turn to cryptographic means of storing data. Encrypting data stored in a database can prevent this disclosure to attackers even if they manage to circumvent the access control mechanism. Thus cryptographic technique can ensure excellent security for databases. Nonetheless the time cost involved in encrypting and decrypting data items can greatly degrade the performance of the database system. A compromise solution must be found between performance and security, by encrypting only sensitive data. In this system the encryption technique considered is Advanced Encryption Standard (AES) and the access control mechanism considered is Role Based Access Control (RBAC).

## 2. Related Work

Denning provided solutions to the security problems of field based protection[4]. Yang, Sesay, Xu, Chen extended the security of database with encrypting attribute and field level using DES and MAC[1]. In this system, we describe the field level encryption using AES and RBAC.

## 3. Role Based Access Control (RBAC)

In RBAC approach, users are granted membership into roles on their competences and responsibilities in the organization. The process of defining role is usually based on analyzing the fundamental goals and structure of an organization. Role can be describes as a named collection of privileges that can be granted and revoked like as single privilege [3]. RBAC is a model for controlling access to resources where permitted actions on resources are indentified with roles rather than with individual subject identities. RBAC can be described in different ways. The most familiar process is a comparison or illustration utilizing the “groups” concept. The concept of group is used to simplify the administration of access control permissions and settings. When creating the appropriate groupings, you have the ability to centralize the function of

setting the access levels for various resources within the general administration of resources taught that is the way to simply the general administration of resources within networks and local machines. However, although the concept of RBAC is the same, it is not the exact the same structure. With the use of groups, general level of access based on a user or machine object grouping is created for the convenience of the administrator. However, when the group model is the used, it does not allow for the true level of access that should be defined, and the entire membership of the group gets the same access. This can lead to unnecessary access being granted to some members of the group.

RBACs allow for a more granular and defined access level, without the generality that exists within the group environment. A role definition is developed and defined for each job in an organization, access control function, with individuals or processes being classified into a role that is then allowed access to the network and to defined resources. This type of access control requires more development and cost, but is superior to MAC in that it is flexible and able to be redefined more easily. RBAC can also be used to grant or deny access to a particular router.

In summary, RBAC is:

- Job based
- Highly configurable
- More flexible than MAC and
- More precise than groups[2]

RBAC include the capability to establish relations between roles, between permissions, and roles and between users and roles. For example, two same user is not allowed to assume both. Roles can also acquire inheritance relations, where by one role inherits permissions assigned to a different role. These role-role relations can enforce security policies, including separation of duties and delegation of authority. Previously, these relations would have required application software encoding, with RBAC, they can be specified once for a security domain.

With RBAC, role permission relationships can be predefined, which makes it simple to assign users to the predefined roles. One of the studies indicates that permissions assigned to roles, unlike user membership in roles, tend to change relatively slowly. The study also found it desirable to let administrators and revoke membership in existing roles without authorizing these administrators to create new roles or change role permissions assignments. One reason for this finding is that assigning users to roles typically requires less technical skill than assigning permissions to roles. Without RBAC, it can also be difficult to determine what permissions have been authorized for what users.

## 4. Advanced Encryption Standard (AES)

Encryption is defined as the transformation of data, via a cryptographic mathematical into a form that is unreadable by anyone who does not possess the appropriate secret key.

There are two types of cryptographic mechanism. They are:

1. **Symmetric cryptography**: where entities share only a common secret key.
2. **Asymmetric cryptography**: where each communication entity has a unique key pair (a public key and a private key).

AES is symmetric encryption algorithm. It is block cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size which can be 128,192 or 256 bits, depends on the number of rounds.

AES has three different versions: they are AES-128, AES-192 and AES-256. However, the round keys, which are created by key-expansion algorithm, are always 128 bits the same size as the plaintext or cipher text block. AES uses several rounds in which each round is made of several stages. Each round uses four transformations; Substitution Bytes, Shift row, Mix Columns, Add Round Key. Each transformation takes a state and creates another state to be used for the next transformation or the next round. The pre-round section uses only one transformation (AddRoundKey): the last round uses only three transformations (Mix Columns transformation is missing.)

### 4.1.1. Rounds in AES

AES uses several rounds in which each round is made of several stages. In AES, the number of rounds to be performed during the execution of the algorithm depends on the key size. The number of round is represented by Nr. The total number of round is always one more than the number of rounds.

$$\text{Number of round keys} = N_r+1$$

The round keys are referred to $K_0,K_1,K_2,\ldots,K_N$.

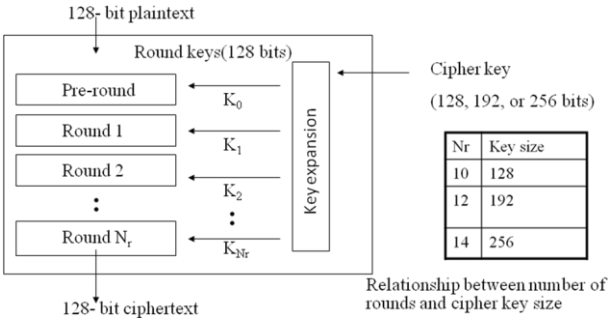


**Figure1:General design of AES encryption cipher**

Figure 1 shows the general design of AES encryption algorithm.

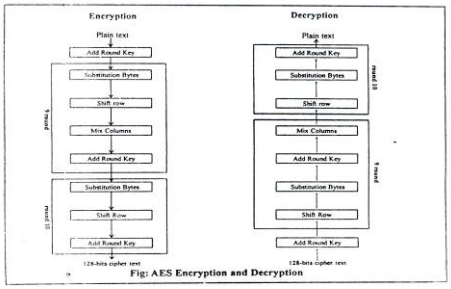


**Figure 2: Design of 128-bit AES cipher and inverse cipher**

Figure 2 shows the 128-bit AES encryption and decryption algorithm.

### 4.1.2. Encryption Algorithm of AES

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr + 1)])
begin
    byte state[4, Nb]
    state = in
    AddRoundKey(state, w[0, Nb-1])
    for round = 1 step 1 to Nr-1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state,
        w[round*Nb,(round+1)*Nb-1])
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w[Nr*Nb,(Nr+1)*Nb-1])
    out = state
end
```

### 4.1.3. Decryption Algorithm of AES

```
InvCipher(byte in[4*Nb],byte out[4*Nb],word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state,w[Nr*Nb,(Nr+1)*Nb-1])
    for round = Nr-1 step-1 down to 1
        InvSubBytes(state)
        InvShiftRows(state)
        InvMixCoulmns(state)
        AddRoundKey(state,
        w[round*Nb,(round+1)*Nb-1])
    end for
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state,w[0,Nb-1])
    out = state
end
```

## 5. Proposed System Design

The proposed system controls the permissions of access by assigning roles. The authorities and permissions are different by roles. The system involves 4 roles and 5 access data. Data involves user, formula, production, product, and factory. Role1 is the highest authority in the whole system. Role1 can do admin level functions such as create and define role of user, insert, update, delete, view. Role2 can perform insert and view functions. Role3 can perform view function and role4 can perform view and comment function. All users possess a unique key. The key is encrypted and stored in database and in a file that exists in a user own storage removable device.

**Table 1: Role, Rank and Access Permission of System**

| User Rank | Role Name | Access Permission | Access Data |
|---|---|---|---|
| Administrator (MD) | Role1 | Create and define role for user, insert,update, delete, view | All data |
| Production Manager | Role2 | Insert, view | Formula, Production, Product |
| Factory Manager | Role3 | View | Factory, Production, Product |
| Marketing Manager | Role4 | View, comment | Product |

Table 1 shows role name, the rank of role and what role can be access to which table by using how access permissions.

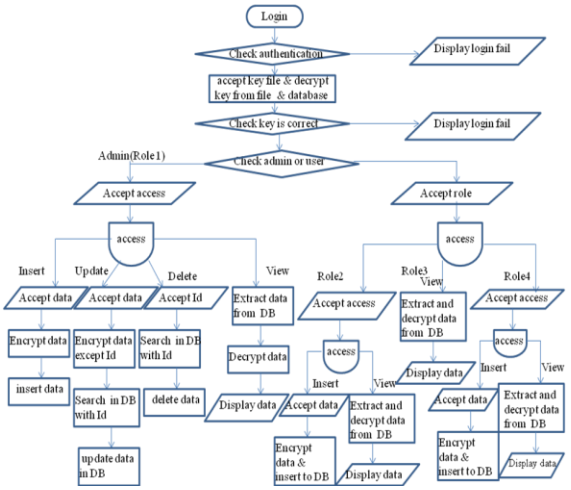


**Figure 3: Process flow diagram of the system**

Figure 3 shows the process flow of the system. In this production system, there are two types of user: administrator and user. Both users can log in the system by user name and password for authentication. If the user name and password is right, the system accepts the url of the key file that is owned by the login user. The system read and decrypts the key from the file by using url and database by using username and password. The two keys are checked whether they are same or not. If the keys are same, this user is identified as a right user, the system permits him to enter and access to the system. If not, the user fails to enter and access to the system.

After permitting the user as a right user to enter the system, the system checks the permitted user is admin or user. If user role is admin(Role1), the user can perform functions such as create and define role for a user, insert , update, delete, view on all user data, formula data, production data, product data, factory data. If user role is Role2 (Production Manager), he can perform insert function on production data that he performed, view function on all formula data, production data that he performed and all product data. If user role is Role3 (Factory Manager), he can view on factory data that he maintains, production data that is performed in that factory and all product data. If user role is Role4 (Marketing Manager), he can view and comment the user feedback from the market on all product data.

In this production system, data are classified into two types: sensitive data and non-sensitive data. Sensitive data are user information, formula information and production information. Non-sensitive data are factory information and product information. So the admin (Role1) can perform all functions on both sensitive and non-sensitive data, the user (Role2) can insert and view on two sensitive data: production data and formula data; and one non-sensitive data: product data. The user (Role3) can view on both two non-sensitive data and the user (Role4) can view and comment on only non-sensitive data: product data. All data are stored in database. Only the secret key is stored in file. Sensitive data are stored with encrypted form and non-sensitive data are stored with plain text form.

When admin creates a user, the system generates the secret key by randomly and encrypts that key and stores in database and in server as a key file. After the admin is creating the user, admin downloads the key file from the server and give that key file to the owner created with user name and password.

When admin and user (Role2) performs insert function on sensitive data, the system firstly encrypts the inputted data and then the encrypted data are stored into the database. When the admin performs update function on sensitive data, the system firstly searches and extracts the encrypted data from the database using the id of data and then decrypts the encrypted data to the plain text and shows to the user. After the user has updated the data, the system firstly encrypts the updated data and then the encrypted data are stored into the database. And vice versa when sensitive data is read, the system firstly decrypts the encrypted data to the plain text and shows the plain text data to the user. When the admin performs delete function on both sensitive data and non-sensitive data, the system searches the deleted data with id of data and then deletes the data from the database.

When both admin and user performs insert, update, delete, view function on non-sensitive data, the system performs only insert, update, delete, view process with database without performing the encryption and decryption process.

This production system uses 128-bit AES algorithm to encrypt/decrypt the sensitive data. Where the sensitive data is less than the 16-byte block size of AES, the data is replicated as many times as necessary to fill the block. If the data however exceeds the block size, the system partitions as a 16-byte data block that is used AES algorithm by chaining with initial data. And then the data is put as input to the AES encryption/decryption algorithm.

In this system, the database used is MySQL Server 2005 Database.

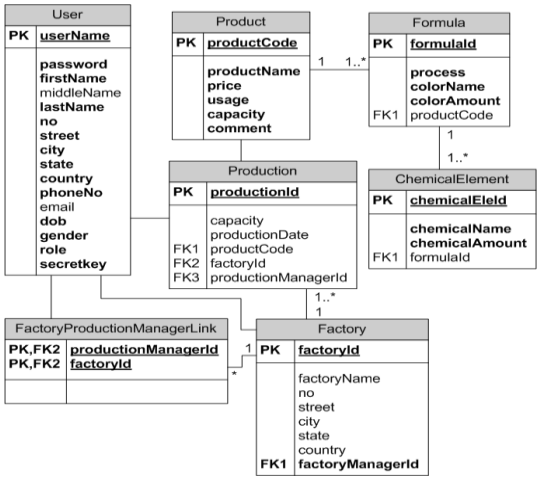


**Figure 4: Database design of the system**

Figure 4 shows database design of the system. In the database, there are 7 tables: User, Product, Formula, ChemicalElement, Production, Factory, FactoryProductionManagerLink table. In User table, there are 16 fields: userName, password, firstName, middleName, lastName, no, street, city, state, country, phoneNo, email, dob, gender, key. The userName refers as the user's id, password refers as the user's password, the firstName refers as the first word of the user's name, middleName refers as the middle word of the user's name and lastName refers as refers as the last word of the user's name, no, street, city, state, country refer to the user's address, phoneNo and email refer to the contact of the user, dob refers to the date of birth of the user, gender refers to the gender type of user, role refers to the user's role, secretkey refers to the secretkey of the user to enter the system. In Product table, there are 6 fields: productCode, productName, price, usage, capacity, comment. The productCode refers as the id of product, the productName refers as the product's name, the price refers as the price of the product, the usage refers as the usage direction of the product, the capacity refers as the package capacity of the product and the comment refers as the comment of the marketing manager for the product. In Formula table, there are 5 fields: formulaId, process, colorName, colorAmount, productCode. The formulaId refers as the id of the formula, the process refers as the step by step process description of performing a production, colorName refers to the type of color of a production, colorAmount refers to the amount of color involves in production and the productCode refers to the product id that the formula is used. In Production table, there are 6 fields: productionId, capacity, productionDate, productCode, productionManagerId, factoryId. The productionId refers to the id no of the production, the capacity refers to the amount of capacity of production that is produced, the productionDate refers to the date of production that produced, the productCode refers to the product id for which the production is performed, factoryId refers to the factory id where the production is performed and the productionManagerId refers to the manager who performs the production. In ChemicalElement table, there are 4 fields: chemicalEleId, chemicalName, chemicalAmount and formulaId. The chemicalEleId refers to id of chemical element, chemicalName refers to the chemical element's name, chemicalAmount refers to the amount of chemical element involved and the formulaId refers to the id of formula in which chemical elements are used. In Factory table, there are 8 fields: factoryId, factoryName, no, street, city, state, country, factoryManagerId. The factoryId refers to the id of factory, the factoryName refers to the name of the factory, no, street, city, state and country refer to the address of the factory and the factoryManagerId refers to the factory manager who has to maintain the factory. In FactoryProductionManagerLink table, there are 2 fields: productionManagerId and factoryId. The productionManagerId refers to the productionManager who works in the specific factory, which is referred as the factoryId. Because in each factory, there are one or more production managers exist.

As mentioned above, this production system uses the Role Based Access Control mechanism to control the access of user to prevent the unauthorized disclosure of information and Advanced Encryption Standard algorithm to conceal the data with encrypted form when the intruder penetrates the database and searches the data that he wants to gain or modify.

## 6. Conclusion

The system used role based access control mechanism to check authorized user, perform user level and administrator level functions. By dividing privilege into roles, the administrator is able to control what access a person has based on the role associated with their user account. So RBAC is very useful in the organization which performs duties and authorities by role and rank. The useful of RBAC is more significant if the system is more and more large. As RBAC is very useful for an organization, cryptography is also useful in storing of sensitive data. In a database system, sensitive data stored in clear form can be easy to attack. However, if the sensitive data are encrypted before storage in the database, the risk from security leaks which attackers can use to penetrate the database can be

eliminated. Therefore by using the combination of these two security mechanism, the system is more secure than the other system that uses only one security system. And to reduce the time spent on encryption and decryption, the system specifies the database into sensitive and non-sensitive data. This makes the time cost for their encryption and decryption to have less significance on the performance of the system.

## 7. References


[1] Zongkai Yang,Samba Sesay,Jingwen Chen and Du Xu. "A Secure Database Encryption Scheme": ISSN 1546-9239, Asian Network for Scientific Information,2004

[2] Cross, Micheal; L.Johnson, Jr, Norris; Piltzecker, Tony; J.Shimonski, Robert and Littlejohn Shinder, Debra.

[3] dosc.rinet.ru/08/glossary.html

[4] Denning, D.E., 1983. Field Encryption and Authentication, Proc. Of CRYPTO 8.9.

[5] Hilchenback, Burkhard, 20th NISSC Proceeding, Baltimore,MD. "Observations on the Real-World Implementation of Role Based Access Control", 1997

[6] Carter, B.,Kassin, A. and Magoe, T. "Advanced Encryption Standard", Germany,October 30,2007

[7] http://cscr.nist.gov/encryption/aes/rijndael

[8] Daemen, J. and Rijmen, V. "Advanced Encryption Standard Choice Is Rijndael", Vol.48, No.1, January 2001

[9] Elisabeth Oswald, Joan Daemen, Vincent Rijmen, "AES-The State of the Art of Rijndael's Security", 2002