International Journal of Engineering & Technology, 7 (4) (2018) 5105-5107

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.25223
Research paper

Analysis of data security for hospital management using data transparent encryption and role based access control

Dr Kamalakannan Machap [1] *, Dr Mohamed Shabbir Hamza Abdulnabi [1], Thiyagu Ravichandran [2]

[1] School of Technology Faculty of Computing Engineering and Technology Asia Pacific University of Technology and Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[2] Bachelor of Science (Hons) in Cyber Security Faculty of Computing Engineering and Technology Asia Pacific University of Technology and Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
**Corresponding author E-mail: drmkamalakannan@gmail.com*

Abstract

Currently, the issue of security is a key concern for organizations, especially those operating within the healthcare sector. The authors thus propose to enhance the integrity of existing healthcare systems through the incorporation of an essential security layer that involves encryption techniques to avoid data leakage or misuse by third parties. Unlike other sectors, a number of healthcare organizations are still reliant upon traditional paper based systems, although the use of electronic patient record systems is steadily growing. The benefits provided by computerized online patient records is offset by the increased risk of unauthorized access to the personal information of the patients. The encryption technique proposed aims to ensure patient medical data is encrypted and safe in the event the storage media or data file is stolen. Furthermore, the developer has used Role Based Authentication Control (RBAC) to assign permissions to roles and roles to users. These roles correspond to positions in an organization and align with the duties of a particular position. In addition, other than encryption techniques the developer has used the MD5 hashing technique to hash and store username and passwords in a hexadecimal character. This increases adds an extra level of difficultly for an authorized individual to access the information in the database. The authors have also implemented additional security features during the login process, thus access to the system is contingent upon the user successfully passing through all of the security procedures.

***Keywords**: Transparent Data Encryption; RBAC; MD5; Discretionary Access Control; M-RBAC; M-Patient-Centric-ABAC.*

1. Introduction

This research paper concerns the development and implementation of Hospital Data Security Management (HDSM). The aim of this proposed system is to ensure patient privacy, and confidentiality, while ensuring that the integrity and security of the proposed system. System integrity and patient confidentiality will be facilitated through the inclusion of more robust Access Control (AC). Moreover, with current technology the information of the patients can potentially be easily accessed by an unauthorized user, leaving the data susceptible to misuse.

2. Scope of research

2.1. Data encryption standard

Data encryption standard (DES) is implemented in the proposed system to ensure the data is protected and also to prevent an unauthorized individual from misusing the confidential information such as a patient's medical report. The developer takes DES into consideration because it works as a main role in protecting the data. DES encryption allows the users to protect their data by translating it into incomprehensible to any person who is not allowed to undo the encryption.

The data encryption standard (DES) is block chipper where cryptographic key and algorithms are applied to a plaintext blocks of a fixed size 64-bit blocks. By using DES, the proposed system can be immunized against brute force attacks, whilst the number of rounds used to encrypt the message prevent the hacker from cracking it. The developer can use DES as a tool to encrypt the data from the input of the user and converting it into hash value.

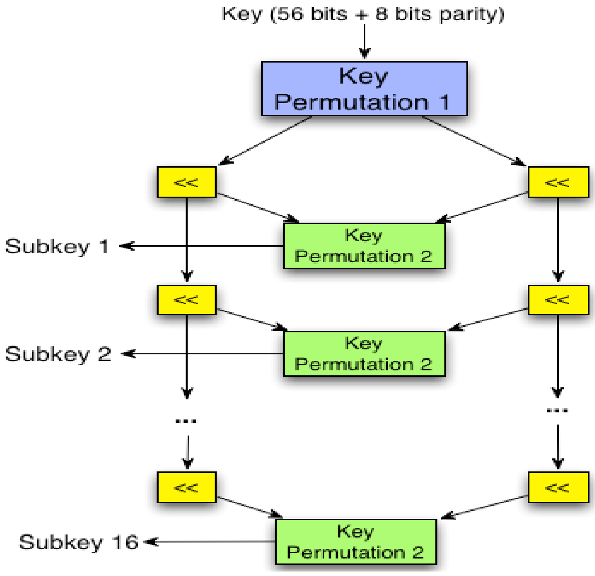

Fig. 1: How the Data Encryption Works.

2.2. MD5 cryptographic hash value

The developer can use MD5 that produces hashes that are 128bits in length, expressed as 32 hexadecimal characters. The Message Digest 5 (MD5) was introduced in 1991 by Ronald Rivest. MD5 helps the developer to hash the data such as the patient's medical information and also hash the string of characters such as the password. Each time the user hashes the same data, the user will get the similar hash value as output and all the data are different sizes but the hashes are similar length.[CITATION Tip14 \l 1033].
MD5 can be used for storing passwords so that upon the creation of a user password it goes through a hashing process to ensure that it is the hash value and not the actual password which is stored. Basically, it will not capture what the user typed and the password will be stored in a hash value. If the user wants to log in again it will hash the user's input and compare with the stored hash value. If the user fails to log in then the hash value did not match with the stored hash value. The developer can use this algorithm to hash the important data and passwords of the patients. [CITATION Tip14 \l 1033].

The developer can use MD5 for database searching where it speeds up the process of searching through database. It can create a hash value for every name on the database list. If the hash value is shorter than the average name, then it will be faster and the computer will search the hash value instead of searching the actual name. [CITATION Tip14 \l 1033].

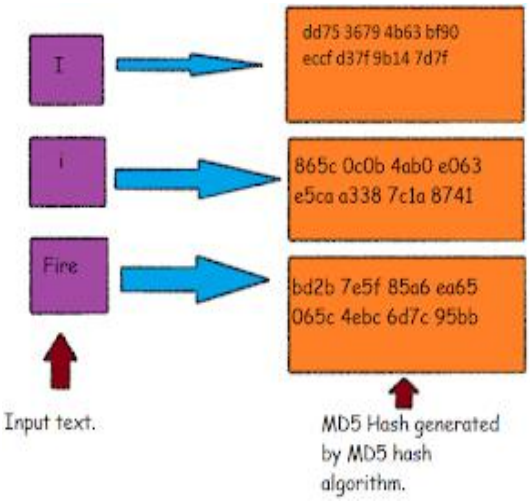

Fig. 2: How MD5 Algorithm Works.

2.3. Role based access control

There are a few access control models which were taken into consideration for the patient's privacy, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). Role-Based Access Control has become one of the most widely recognized access control models and is considered especially appropriate for medicinal services system. RBAC is based on the concept of assigning permissions to roles and roles to users. Roles frequently correspond to positions in an organization and roles play an important part in performing the duties of a particular position. [CITATION Lil09 \l 1033].

In the temporal stage, the temporal component will allow the management of access right depending on the time condition. The permission component will allow the specification of the access right where it defines which operations are permitted on various objects. The list is related to the system user and permission, where this model is divided to indicate the users who have the authority to access the system. The purpose component will limit document access to the listed purposes only. Moreover, the authors have chosen a model which is multilevel because a hospital system will have multiple control levels such as Bell-LaPadula model. [CITATION Mar13 \l 1033].

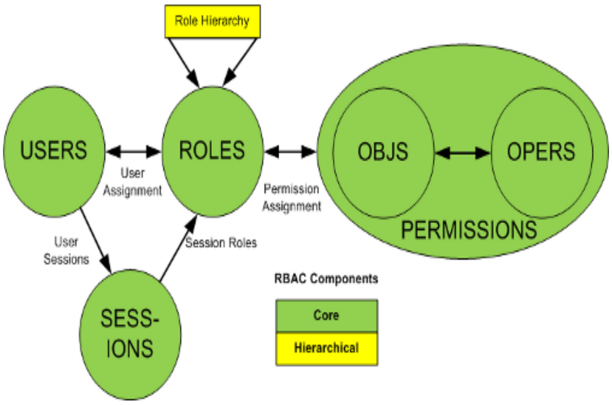

Fig. 3: Role Based Access Control.

There are three steps that the authors have chosen for access control in the proposed system, these are Multi Level RBAC model (M-RBAC), Multi-Level Purpose (MP-RBAC) and M-Patient-centric-ABAC (MPP-ABAC). The Multi-Level RBAC is the expansion of the MAC and RBAC which has the ability to delineate between different the levels of security. A medical document could thus be categorized depending on the level of privacy required using nomenclature such as top secret, secret and normal. The top-secret level will allow access only to the patient that the author of the document decrees, whilst the secret level might allow access to the patient or doctor. [CITATION Mar13 \l 1033]. The normal level could have controls as in the RBAC model. In fact, through this model it is possible to associate operations on objects to roles set by the healthcare organization.

In the Multi-Level Purpose stage, the level of privacy is considered normal and is extended from the M-RBAC. It allows the management to guide the patient through the security policies and also provides supports for highly complex privacy related policies, highlighting purpose and obligations. [CITATION Fuc10 \l 1033]. Furthermore, it allows the user to access the system in the case of emergency through the help of features component which allows the user to associate particular attributes to the roles.[CITATION Mar13 \l 1033].

In the final step which is M-Patient-centric-ABAC, the patient will be provided with the opportunity to directly manage the access policies regarding their personal medical documents. Through this component, the users are allowed to define their own policies by allowing or denying access to their documents for a specific individual and for a given purpose. Additionally, this component allows the user to choose a purpose which is predefined in the system and which the user wants to associate to their documents. [CITATION Mar13 \l 1033]. Through this model, the system can identify which users have permission to access through the relationship of Able and Unable.

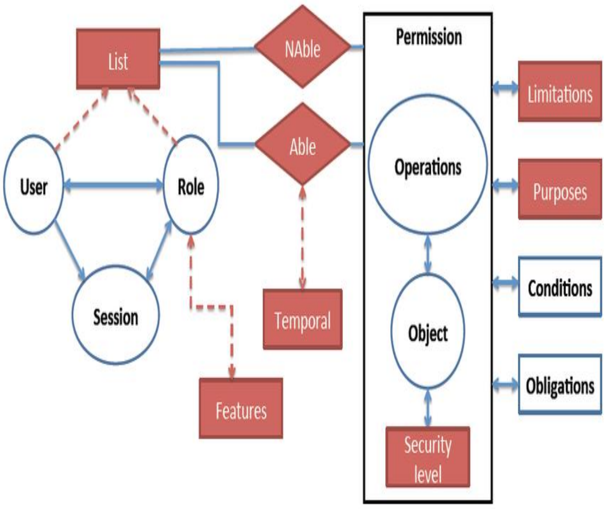

Fig. 4: MPP-RBAC Model: [CITATION Mar13 \l 1033].

3. Significant of research

3.1. Transparent data encryption

Transparent Data Encryption (TDE) allows the user to encrypt their sensitive data, such as medical information or finance related details, which store in table and table spaces. Developers can use TDE to protect the patients' medical details from an unauthorized individual. By applying this technique, the encrypted data will transparently decrypt for an authorized user when they access the data. The authors will implement this technique to make sure the patient's medical data is encrypted and safe in the event the storage media or data file is stolen.[CITATION ORA18 \l 1033].

Transparent data encryption enables basic and simple encryption for sensitive information in columns without requiring users or applications to deal with the encryption key. There is no compelling reason to utilize perspectives to decrypt data, because once a user has passed essential access control checks the data will transparently decrypted. So, with this technique implemented in the system the authors can ensure that the patient's data on the disk is encrypted and the encrypted data becomes transparent to the system.

Transparent data encryption is a key based access control system. The process cannot execute until authorized decryption occurs even if the encryption process was successfully completed. This technique will therefore only allow the authorized user to access the table. A master key will be created which containing all the keys of encrypted column and stored in a dictionary table in the database to prevent unauthorized use in the system. [CITATION ORA18 \l 1033].

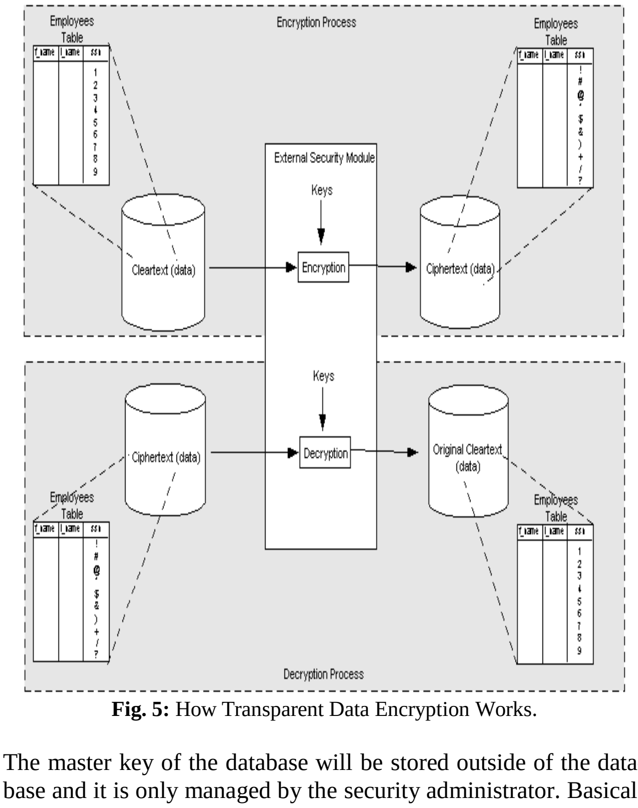

Fig. 5: How Transparent Data Encryption Works.

The master key of the database will be stored outside of the database and it is only managed by the security administrator. Basically, the external security model is stored in such a way because it prevents access by an unauthorized user. Furthermore, to store the master key the encryption keys will be generated to execute the encryption and decryption process. As shown in the figure 4, the external security module divides the ordinary program functions from encryption operations, making it possible to separate their task between a database administrator and security administrator. This will ensure no single administrator is allowed to take control of the complete access to all data. [CITATION ORA18 \l 1033].

4. Future enhancement

In future, the authors would like to enhance the system by incorporating some essential security features, such as image based authentication during the log in process to prevent any robotic or scripting hack from accessing the information. Moreover, the authors would like to implement some biometric features into the proposed system such as facial recognition authentication. The authors can improve the system for future use by implementing the proposed system using cloud based processing.

5. Conclusion

From this paper, the developer has conducted research and analysis into Transparent Data Encryption and how it may be implemented in the proposed system. The paper has also sought to investigate how to limit access to the system's data through the use of Role Based Access Control (RBAC). Role Based Access Control can help the authors to determine what roles, module sessions, and permissions should be implemented in the system. The combination of these techniques will help in the development of a more robust security system and thus help to reduce the risks to patient data.

References

[1] Andrew. (2017). Rational Unified Process. Retrieved from airbrake. PP. 15-19.

[1] Anwar, A. (2014). A Review of RUP (Rational Unified Process). International Journal of Software Engineering.pp.1-17.

[2] Carpenter, M. E. (2017). *Pocket Sense*. Retrieved from pocketsense.com: https://pocketsense.com/advantages-and-disadvantages-of-electronic-claims-and-patient-files.

[3] Diachenko, B. (2017, October 10). Mackeeper Security Research Centre.pp. 54-68.

[4] Fuchs, L. (2010). Methodology for Hybrid Role Development.pp.16-21.

[5] Fund, R. L. (2018). Literature reviews.pp.27-34.

[6] Mario Sicuranza, A. E. (2013). Access Control Model for easy management of patient privacy in EHR system.pp.8-12.

[7] Martell, M. (2017). Always Encrypted (Database Engine).pp. 24-33.

[8] Mudit_Agarwal. (2008), Security Features Analysis for ASP.NET.pp7-9.

[9] ORACLE. (2018). Database Advanced Security Guide.pp.4-8.

[10] Practo Technologies. (2016). Insta Hospital and Clinic Management.

[11] Røstad, L. (2009). Access Control in Healthcare. Trondheim: NTNU.pp.54-63.

[12] Saikumar, I. (2017). DES- Data Encryption Standard. *International Research Journal of Engineering and Technology (IRJET)*, 6.

[13] Tiptop Security. (2014, December 15). Tiptop Security. Retrieved from what is a Cryptographic.pp. 6-9.

[14] Wavemaker. (2018). *Rapid Application Development vs. Traditional SDLC.*