Advanced Science and Technology Letters
Vol.78 (MulGrab 2014), pp.95-98
http://dx.doi.org/10.14257/astl.2014.78.19

Personal Information Encryption Technique based on Cryptographic Equipment in SAP ERP Systems

Hyo-ju An[1], Wan-Sup Cho[2], Yeong-real Kim[2]
[1] Department of Business Data Convergence
[2] Department of Management Information Systems
Chungbuk National University
keep5t@nate.com, {wscho, yrkim}@chungbuk.ac.kr

Abstract. Due to the enforcement of the Personal Information Protection Act, businesses should perform the encryption for ensuring the stability of the important data in the ERP system. This study proposes an encryption method to apply the token encryption scheme that can perform the encryption without applying the changes to the database schema, allow users to use it more easily and conveniently, and to enhance the efficiency of business operation with the SAP ERP system most commonly used in the world.

Keywords: Personal Information Protection Act, SAP ERP, token encryption

1 Introduction

With the development of the Internet, there have been and rapid increase in crimes and damages related to the personal and corporate information leakage. For the prevention of the information leakage accidents, the Personal Information Protection Act was enforced in September 2011, and businesses have been taking physical and technical security measures for the protection of personal information and important data. The study investigates characteristics of the database in the SAP ERP system most commonly used in Korea and proposes an encryption method so that users can take advantage of the encryption of the personal information and important data more efficiently through the application of the token encryption scheme that can perform encryption in the SAP package system using a separate hardware device.

2 Related Work

Since SAP system features package software that has restrictions that do not allow the database object changes, it cannot be encrypted with a general DB encryption method. In consideration of characteristics of the SAP database, a tokenization technology is used as a SAP database encryption technique. The tokenization technology replaces the data to be protected with a token and uses the token with a unique value and the same data type and length instead of the original data. Methods for generating a token include a random number generation method and FPE method.

ISSN: 2287-1233 ASTL
Copyright © 2014 SERSC

3 Empirical Research Design

The encryption/decryption system presented in this study is composed of a user screen (SAP GUI), a SAP server, an encryption server and a cryptographic device.

3.1 Encryption process

① Plaintext input

An administrator enters personal information through the SAP GUI or requests the encryption of the personal information field stored in the SAP database table.

② Request for encryption

The personal information data sent from the SAP GUI is transmitted to the encryption server using a function module.

③ Encryption implementation and storage

The transmitted personal information data is encrypted by the hardware device in the encryption server and stored in the encryption server database after generating a token, which is a corresponding random value. In the hardware equipment, AES or ARIA encryption algorithm is used.

④ Encryption value transmission and storage

The token value and cipher text generated by the result of the function call are stored in the encryption server, and only the token value is transmitted to the SAP server and stored in the SAP database.

3.2 Decryption process

① Token input

An administrator enters a token through the SAP GUI or requests the decryption of the token stored in the SAP database table.

② Request for decryption

According to the presence and absence of administrator's decryption right, the decryption of the entered token is requested through the function module in case of the presence of the right. However, in case of the absence of the decryption right, the process terminates without proceeding with the decryption process, and the message of no rights displays.

③ Implementation of search and decryption

If there is the corresponding value after searching the data that is matched with the token, the cipher text is decrypted through the hardware equipment.

④ Plaintext transmission and output

The encryption server transmits the decrypted plaintext as the result value of the function call and displays the decrypted data in the SAP GUI screen. The decrypted personal information data is not updated to the SAP database.

 Copyright © 2014 SERSC

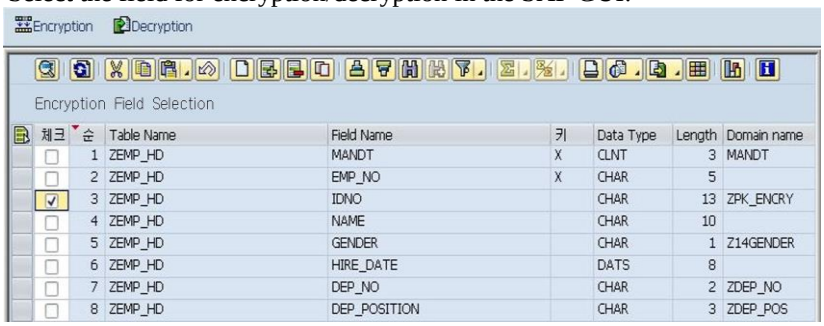
3.3 Proposed system

(1) Proposed system operation procedures

Step 1. DBA and DB authorized person selects data for encryption/decryption.

Step 2. Input/select the table for encryption/decryption in the SAP GUI.

Step 3. Select the field for encryption/decryption in the SAP GUI.



체크	순	Table Name	Field Name	키	Data Type	Length	Domain name
☐	1	ZEMP_HD	MANDT	X	CLNT	3	MANDT
☐	2	ZEMP_HD	EMP_NO	X	CHAR	5	
☑	3	ZEMP_HD	IDNO		CHAR	13	ZPK_ENCRY
☐	4	ZEMP_HD	NAME		CHAR	10	
☐	5	ZEMP_HD	GENDER		CHAR	1	Z14GENDER
☐	6	ZEMP_HD	HIRE_DATE		DATS	8	
☐	7	ZEMP_HD	DEP_NO		CHAR	2	ZDEP_NO
☐	8	ZEMP_HD	DEP_POSITION		CHAR	3	ZDEP_POS

Step 4. Perform encryption/decryption in a batch processing.

Step 5. Check/verify the encrypted/decrypted data.

MANDT	EMP_NO	IDNO	NAME	GENDER	HIRE_DATE	DEP_NO	DEP_POSITION
900	14001	(ds>a4}u&Z8qG	S. J. LEE	F	2013.09.01	01	P80
900	14002	yI&I1jYmBwvf|	S. R. HONG	F	2013.09.02	02	P70
900	14003	NSi.]₩$4./mK,	D. C. MHA	M	2013.09.03	03	P10
900	14004	5MOx"AmiXLEen	S. Y. PARK	M	2013.09.04	04	P70
900	14005	s$5>z9=5,KJq)	A. B. PARK	M	2013.09.05	05	P80

(2) Three measures for the proposed system

[Table 1] Features of three measures for the proposed system

SEGMENT	INSERT	UPDATE	DISPLAY
Business perspective	Registration of new employees	Modification of employee information	Inquiry about detailed information of employees
Program modifications in performing encryption/decryption	X	X	X
Table structure modifications in performing encryption/decryption	X	X	X

① INSERT PROCESS

At the time of employee information input, the personal information data is encrypted and then stored after being changed into the token value.

② UPDATE PROCESS

In the case of the authorized person, the token value is decrypted, and the source of the personal data is output. In the case of the unauthorized person, the right for modification of employee information is not given. If there is a change in the number of the social security number, the existing token value is changed into a new token value and stored.

Copyright © 2014 SERSC

③ *DISPLAY PROCESS*

Employee information header table and employee information item table are joined. In the case of authorized the person, the token value is decrypted, and the source of the personal data is output. In the case of the unauthorized person, the token value is output and shown.

4 Conclusion

This study was conducted by using an encryption module with a built-in token encryption algorithm, targeting the SAP package system that has a characteristic of maintaining the properties of the original data without changing the structure of the database. It constructs the encryption function module by synthesizing various situations that can have an access to the database in the practicalaffairs of SAP, thereby proposing a scenario. Since the encryption can be performed using a simple click through the GUI for an exclusive use, it can not only improve user's convenience and enhance the efficiency of the business operations.

Acknowledgments. This research was supported by the MSIP(The Ministry of Science,ICT and Future Planning), Korea, under the "SW master's course of a hiring contract" support program (NIPA-2014-HB301-14-1011) and ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1022) supervised by the NIPA(National IT Industry Promotion Agency)

References

1. Kim, Myung-soo, SAP cryptographic implementation and operation. Korea Micro Software, February issue (2002)
2. Lee, Bu-hyeong, Comparison and performance evaluation of database encryption techniques. Master's thesis at Seoul National University of Science and Technology (2013)
3. Park, Gyeong-soo, Token Encryption Techniques Using Hardware Equipment for ERP Systems, MS Thesis, Chungbuk National University, 2014.
4. Hwang, Chi-ha, Park Jun-seong, Choi Jae-woo, Kim Hak-byeong, A study on the SAP DB encryption. Journal of Information Security, Vol. 23, No. 1, pp.61--67 (2013)
5. Kim, Yeong-ryeol, A strategy for implementing educational virtual enterprises for SAP ERP system training. Journal of Korea Society of Industrial Information Systems, Vol. 16, No. 1. pp.49--58(2011).
6. Lee, Soo-gyo, A study on the optimal encryption method in the package software environment. Master's thesis at Korea University (2012).
7. Go, Gwan-yong, A study on the measures for strengthening the efficiency of personal information collection and management. Master's thesis at Dongguk University (2012).
8. Hong, Jeong-wha, An empirical case study on the performance due to the database encryption. Master's thesis at Korea University (2011).

 Copyright © 2014 SERSC