ISSN: 2458-8989

Natural and Engineering Sciences

NESciences, 2018, 3(2): 207-224 doi: 10.28978/nesciences.424677

- RESEARCH ARTICLE -

Using Record Level Encryption for Securing Information in Classified Information Systems

Blerim Rexha, Halil Sadiku, Bujar Krasniqi[*]

Faculty of Electrical and Computer Engineering, University of Prishtina, Prishtina, 10000, Kosovo

Abstract

Information technology (IT) systems have great potential to improve the efficiency and methods of operation in each government organization, providing added convenience and flexibility. Currently, most of government law enforcement agencies have digitized their methods of work by advancing their user services. With this new approach, have come new threats, therefore, it is necessary to develop and implement standard policies to enhance information security and privacy on all classified information systems. In this paper a novel solution is presented for protection of information up to the record level encryption by applying the Advanced Encryption Standard (AES) algorithm using derived symmetric master key. The master key is unique per each record and is calculated in the client application. The uniqueness of the derived master key is assured by applying the exclusive or operation of the key of each record and the unique key of the client. Furthermore, this paper includes a critical approach on existing cryptographic methods and proposes additional methods to protect information, such us authentication, access control, and audit.

Keywords:
Information security, Privacy, Encryption, Decryption, Access control, Audit

Article history:
Received 20 January 2018, Accepted 09 May 2018, Available online 14 May 2018

Introduction

Improving the quality of services through IT systems is one of the top priorities of government law enforcement agencies in each democratic country. This is also confirmed by the European Commission (EC) with an implementation plan for e-government systems. The EC has come up

[*] *Corresponding author: Bujar Krasniqi, e-mail: bujar.krasniqi@uni-pr.edu*

with a recommendation to extend the digital transformation of all government activities and services in the period 2016 to 2020. However, the greatest concern of those systems is the security and privacy of information (European Commission, 2016).

Seeing the increasing trend of cyber-attacks, the weaknesses in security can cause great damage to the institutions with unpredicted costs, depending on what the goals of the attacks were. Usually, classified information systems that are stored unencrypted in databases are the main focus of such attacks, especially in governmental law enforcement agencies.

Securing information systems with firewalls, storage encryption, or access control is insufficient. It is possible that the risk will be greater if we expose classified information to "reliable" internal parties, such as database and security administrators, contractors, or any other party. Therefore, special importance should be paid to internal security by prohibiting the misuse of classified information by authorized and unauthorized parties. According to legal requirements, all information systems must apply cryptographic functions for securing all classified information in case they come into the possession of the "bad" people.

Assuring confidentiality (privacy) is one of the main objectives of cryptographic functions (Menezes at al., 1996), as well as one of the main challenges of classified information systems. Formal encryption of data with a single key does not provide the required level of confidentiality for classified information systems. Encryption must be provided in an independent form from all parties and should be controlled only by the system, thus preventing the decryption of data from cyber-attackers or even from system administrators. Other important issues that need to be addressed carefully in these information systems are authentication, access control, and audit.

The main purpose of this paper is to enhance the security of classified information systems for government law agencies by eliminating the risks of manipulation with classified information by all parties, including system administrators. To fulfil this requirement, at the record level encryption, a novel information system was developed. The developed information system prototype was named Criminal Case Management System (CCMS). Each record in the database is encrypted with a unique derived master key, which is the exclusive or operation of the key of each record and the unique key of the client. Access control is provided for all components of the client application, as well as in the data level. The audit process registers all the activities within applications, and all activities which are stored directly in the database.

State of the Art

Classified information, as defined by each country's legal framework, is information of national importance for those countries. An example is the classification of information for all European Union (EU) countries in four levels (European Commission, 2015):

- TOP SECRET,
- SECRET,
- CONFIDENTIAL,
- RESTRICTED.

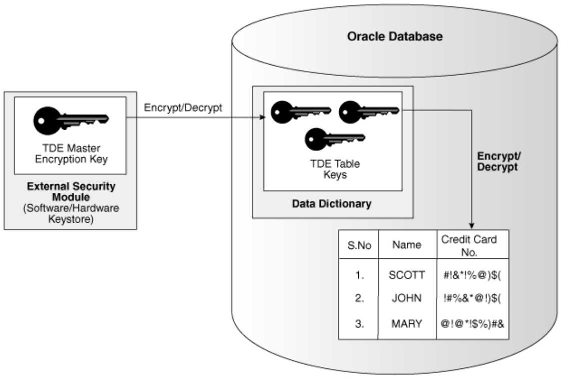
Based on the regulation for classification of information in EU countries, information classified as RESTRICTED will automatically be declassified after thirty years (European Commission, 2015).

Many solutions so far have been proposed for data encryption in the database level, such as Bouganim and Guo (2009), Arshad at al. (2007), Aarthi and Ramaraj (2012), Huey (2017), and Varga at al. (2016). “Database Encryption” is one of the approaches, which tends to define data encryption at the database level using a hardware security module (HSM) (Bouganim and Guo, 2009). The hardware module performs the encryption and decryption of data, while data is stored on the encrypted database server. It does not support point-to-point encryption. Query results are delivered in plaintext from HSM to client, which can be easily intercepted through a traffic analyzer. HSM is managed by a security administrator, who can decrypt data with close collaboration with the database administrator.

A similar solution, proposed by Arshad at al. (2007), provided the storage of each user's key in the application server file. This key was protected by the user's password that was stored in the system database. Since administrators have access in both servers and the way through which the password is created is known, then the decryption of client records is not an “impossible" process. Another approach was presented in Aarthi and Ramaraj (2012), where the encryption key was generated automatically based on the number of the table, the row, and the column. Decryption is an easy process because the decryption key for each row is known.

Solutions for securing database records were also provided by corporations such as Oracle and Microsoft, as part of their products for Database Management Systems (DBMS) (Huey, 2017; Varga at al., 2016).

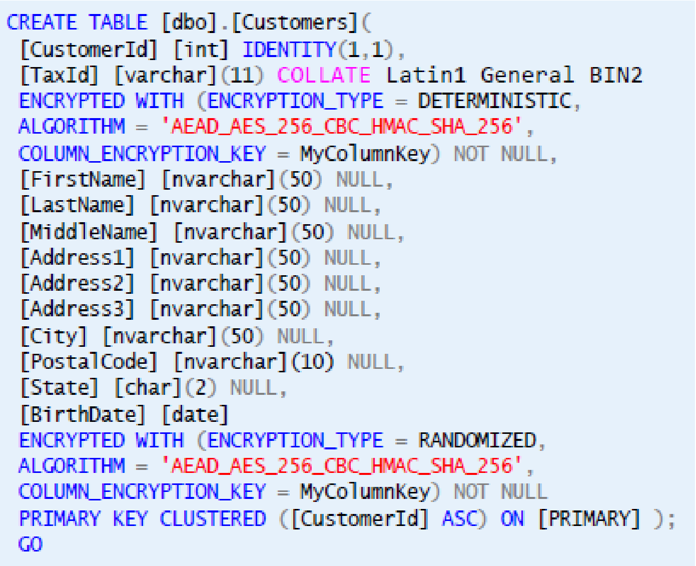
Oracle Database Release 1, version 12.1.0.2, has advanced capabilities of Transparent Data Encryption (TDE) (Huey, 2017). It provides encryption keys, which can be used to encrypt one or more columns inside of one table. Encryption keys are stored in a single TDE table key, as presented in Figure 1. A TDE master key is used to protect (encrypt) all encryption keys, which is stored in an external security module.


Oracle Database
TDE Master Encryption Key
External Security Module (Software/Hardware Keystore)
Encrypt/Decrypt
TDE Table Keys
Data Dictionary
Encrypt/ Decrypt

S.No	Name	Credit Card No.
1.	SCOTT	#!&*!%@)$(
2.	JOHN	!#%&*@!)$(
3.	MARY	@!@*!$%)#&

Figure 1. TDE encryption (Huey, 2017)

Always Encrypted is an encryption service in MSQL Server 2016, which functions in the same way as the TDE of Oracle database 12.1c. Here the column master key is stored in a trusted key store, such as Windows Certificate Store, or in a hardware security module. Column encryption keys are saved in the database as metadata (Varga at al., 2016). First, a column master key has to be created, which then can be used to create encryption keys. However, the database administrator knows the column's encryption key used to encrypt each column data. While creating a table one has to assign the encryption key of a column, as presented in Figure 2.



```
CREATE TABLE [dbo].[Customers](
 [CustomerId] [int] IDENTITY(1,1),
 [TaxId] [varchar](11) COLLATE Latin1 General BIN2
 ENCRYPTED WITH (ENCRYPTION_TYPE = DETERMINISTIC,
 ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256',
 COLUMN_ENCRYPTION_KEY = MyColumnKey) NOT NULL,
 [FirstName] [nvarchar](50) NULL,
 [LastName] [nvarchar](50) NULL,
 [MiddleName] [nvarchar](50) NULL,
 [Address1] [nvarchar](50) NULL,
 [Address2] [nvarchar](50) NULL,
 [Address3] [nvarchar](50) NULL,
 [City] [nvarchar](50) NULL,
 [PostalCode] [nvarchar](10) NULL,
 [State] [char](2) NULL,
 [BirthDate] [date]
 ENCRYPTED WITH (ENCRYPTION_TYPE = RANDOMIZED,
 ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256',
 COLUMN_ENCRYPTION_KEY = MyColumnKey) NOT NULL
 PRIMARY KEY CLUSTERED ([CustomerId] ASC) ON [PRIMARY] );
 GO
```

Figure 2. Always encrypted columns (Varga at al., 2016)

Both technologies, Oracle and Microsoft, encrypt all records of a column with one key. If the key of the column is decrypted, then all data of that column can be decrypted. Also, all processes of encryption or decryption can be managed by the administrator of the database, who can enable or disable the encryption properties inside of DBMS.

Cryptographic functions should not depend on individuals, but should be provided as an independent platform, which must be managed only by the system. Therefore, we propose a novel solution that addresses these issues and takes the above security concerns into account.

Securing Records

Classified information should be stored as encrypted data and in this form must be transmitted over the network, from database to client applications. This procedure provides internal and external security of the information.

To secure records that hold classified information in database, Advanced Encryption Standard (AES) algorithm, in Cipher Block Chain (CBC) mode, is used for encryption. The size of the key is set to 256 bits. Encrypting data with AES algorithm is secure enough and is approved to secure data at rest by National Security Agency (2017). AES is a symmetric encryption algorithm, which uses one secret key to encrypt and decrypt data. However, the challenge about where the secret key will be stored rises. Therefore, we propose a novel approach that derives the secret key, named the master key, which is not stored in the database, but is derived from two other keys within client application.

In Figure 3 the concept of our solution is presented, where each record is encrypted by a unique master key. The encryption and decryption processes are performed at the application level, where the master key is calculated. After each encryption or decryption process the master key is destroyed. Master key (M_{key}) is the “exclusive or” between record key (R_{key}) and client key (C_{key}), as in □□□$_{key}$ = R_{key}□$\oplus$□□C_{key}□ □□□

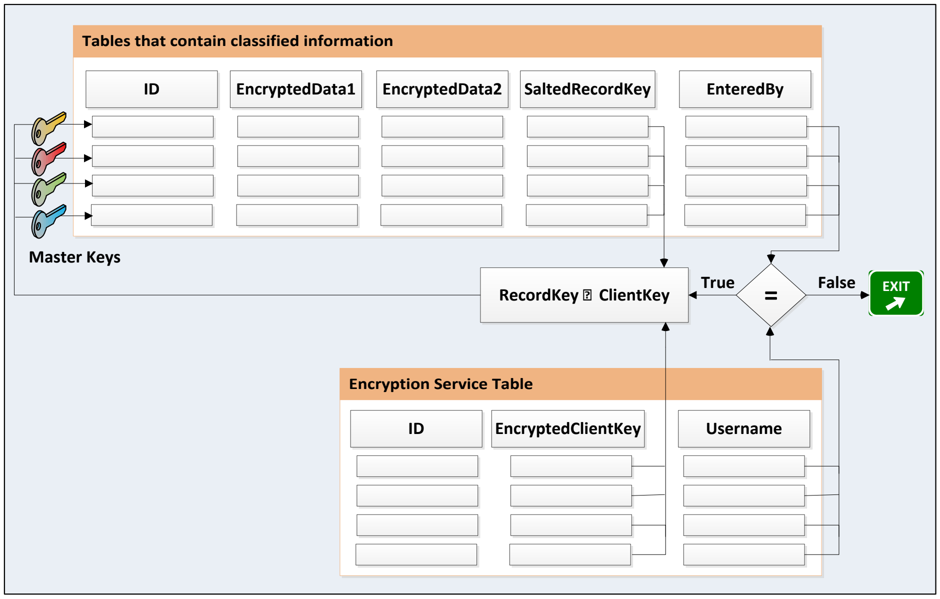


Figure 3. Record level encryption with master key

The client key (AES 256 bit length) is generated when the user account is created in the system administration console. The client key has a static value, which is stored in encrypted form in CCMS database. To generate the client key the Rfc2898DeriveBytes class of Microsoft .NET library is used, which combines Secure Hash Algorithm (SHA 256) bytes of random string, salt (random bytes) and performs 1000 iterations to derive the key. The number of iterations, should be greater than zero, and is set to its default value 1000, as recommended by (Microsoft, 2017). No other tests were performed on this issue, and the count of 1000 iterations was accepted for this application.

Encryption and decryption of the client key is performed by the service of CCMS system using the Rivest, Shamir and Adleman (RSA) algorithm. The issued X.509 digital certificate by the local Certificate Authority (CA) is used by service system to encrypt the client key. While the user is using this information system, the client key is stored in the Random Access Memory (RAM) of the client workstation. An example of implementation of X.509 digital certificate is presented in the solution for Student Management Information System at the University of Prishtina (Rexha at al., 2010). In this case the X.509 digital certificate is stored in the smart card of professors to digitally sign the student grades.

For all classified data a random key (AES 256 bit length) is generated for each record, which is stored in a specific column with all encrypted data of record (as presented in the Figure 3). This key is created before every insert on each table of the database. If data is changed in at least one column from users that did not insert that data, the system will change record key for that record and all data of this record will be encrypted with a new master key.

Bytes of encrypted data in database are stored in the American Standard Code for Information Interchange (ASCII) string format. To convert encrypted data, a Base64 encoding is used, which is one of the most known encoding schemes used for those processes, as well as for the exchange of those data between different software platforms (Josefsson, 2006).

More volume space to store encrypted data is obviously needed. Encrypted data size is larger than unencrypted data, i.e. a plain text with 1081 characters when encrypted using AES with 256 bit key will produce a cipher text with approximately 1580 characters. In order to use the database storage more efficiently we have performed compression on the plain text bytes by implementing the Deflate Compression Algorithm. The format of this algorithm consists of a series of successive input data blocks, that uses the LZ77 algorithm and Huffman coding for data compression. The LZ77 algorithm searches for repeated substrings, and replaces them with backward references occurring in the same or previous input data blocks. Meanwhile, the Huffman coding uses a binary code tree for every symbol, called a leaf node, and assigns a frequency cost, or weight, for every occurring symbol in the input data block (Oswal et al., 2016). As the project is developed in the Microsoft environment, we have used the DeflateStream class provided by Microsoft .NET library.

Based on the example of 1081 characters of plaintext, using compression of plain text bytes, the encryption will produce approximately 856 characters of cipher text, which is a 79% (856 compressed and encrypted byes / 1580 not compressed and encrypted bytes) savings of database storage.

Cipher Block Chain (CBC) mode is used for AES encryption and decryption processes. The reason for using the CBC mode is to create different blocks of cipher text from identical blocks of plain text. But, CBC mode requires the use Initial Vector (IV), which is stored for decryption. IV is not a secret value. In this way, IV bytes are used as salt to secure more data and record key. Table 1 presents the storing method of encrypted data and record key. Before encryption, IV bytes are concatenated with compressed bytes of plaintext. So, concatenated bytes (IV || compressed plaintext) are encrypted, converted in ASCII using base64 encoding, and then stored in in this format in the database. This format is repeated for all columns of each record that contains classified information. Within this process the concatenation of bytes (IV || record key) is done after the encryption process.

Table 1. Encryption method of classified information

Encrypted data 1		**Encrypted data 2**		**Salted Record Key**	
Salt (IV)	Compressed Plaintext1	Salt (IV)	Compressed Plaintext2	Salt (IV)	AES 256 bit Random Key

Key exchange

In order to achieve higher levels of security we adopted the approach of using smart card-based technologies that use public key infrastructure (PKI). According to (Mahajan at al., 2014), smart cards are secure portable storage devices used for several applications, especially security related ones involving access to system's database either online or offline. With the use of smart cards, institutions will enhance security for many processes of systems, especially for authentication and access control. Based on the (Albarqi at al., 2015), PKI is a way of providing security measures by implementing the means of key pairs among clients, which provides X.509 standard certificates for the main cryptography functions such as authentication, confidentiality, non-reputation, and integrity.

Today there are many examples of the implementation of these two components as a comprehensive element in securing information in many aspects. We can emphasize the implementation of smart cards “Common Access Card (CAC)” from the Department of Defense (DoD) of the United States (US) for four million US army personnel within the “DoD Personnel Identity Protection” project (Department of Defense, 2004). This project started as a response to the attacks of September 11, 2001 and was implemented in 2006. Apart from cryptographic functions, CAC cards are used also for physical access control. In the presented solution smart card should be used in the authentication process of users, providing two-factor authentication. Issued digital certificates from Certificate Authority as part of PKI infrastructure should be stored in the smart cards of clients. If a smart card is lost, CA can revoke the X.509 digital certificate that was stored in that smart card.

Therefore, systems that process classified information must use two-factor authentication, where user authentication is done by a smart card and the Personal Identification Number-PIN. Two-factor authentication will enhance security during login process in classified information systems.

Using this two-factor authentication approach, we have developed two applications within CCMS system, client and Windows service application, to assure security during the key exchange process. Client application will use the Windows Communication Foundation (WCF) service to communicate with the database. Communication between these two applications (Client app and WCF service) is secured by Secure Socket Layer (SSL) protocol using the WCF Transfer security feature (Lowy and Montgomery 2015).

Figure 4 presents the key exchange algorithm by which the client key exchange process is managed, ranging from the authentication part of users to the delivery of client key to client application. The establishment of the key exchange undergoes the following steps:

1. The service of CCMS system checks whether the user is registered in the CCMS database to proceed further.
2. If the user exists, credentials are delivered for authentication in directory service. After each successful authentication, system continues with the next step; on failed authentication process, the user can guess the password to connect to the CCMS system a maximum of three times.
3. After successful authentication, the CCMS service receives the encrypted client key from the database and decrypts it.
4. Client application receives decrypted client key together with user authorizations. By this step, the user is connected to the CCMS.

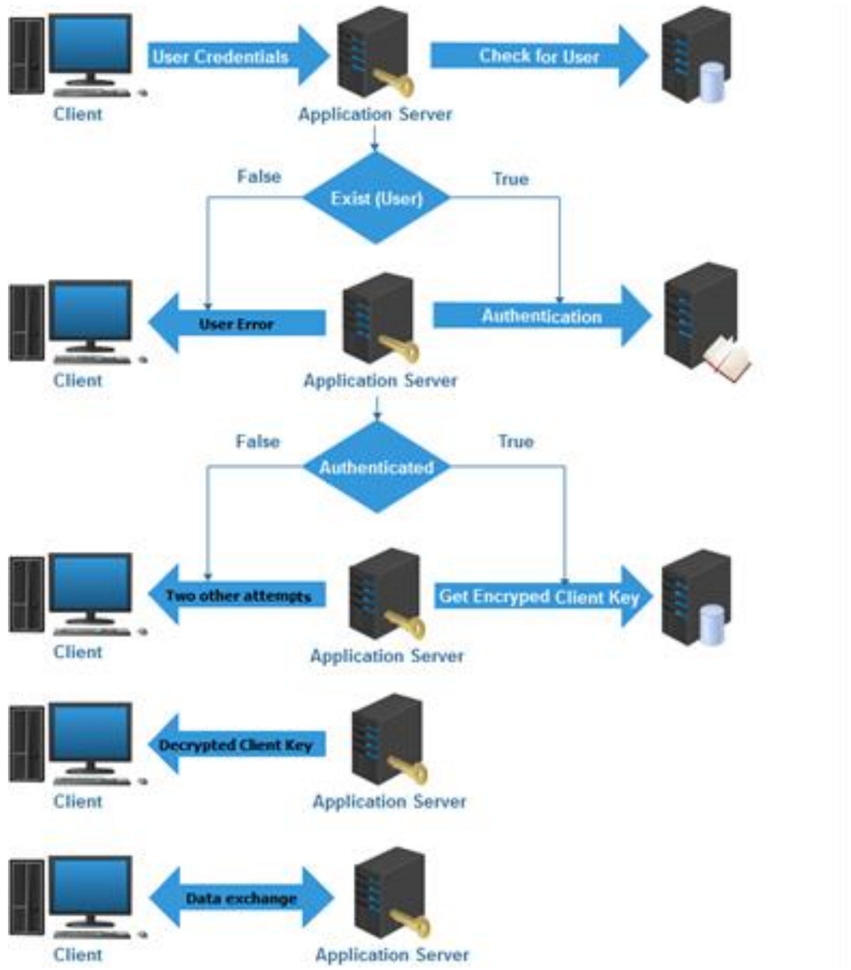


Figure 4. Key exchange algorithm

This interconnection between systems, smart cards, and PKI, is a solid foundation for information security at a wider level. In this way unauthorized access to classified information system is prevented by securing the authentication process in client workstations with two-factor authentication, and exchanging keys in a secure medium with a unique method.

Encryption

The data encryption process is one of the most sensitive parts of each system, from which information security and privacy is depended. In our solution, classified information is stored in encrypted form, and is exchanged as encrypted data from database to client applications. The encryption method with a non-stored key (master key) provides the proper security for classified information systems because the weakest point of each encryption algorithm is the key. Keeping the keys in a safe place is again depended on the security of another key. For this reason, we have created a key management process that is controlled only by the developed system, which prevents the decryption of data from intrusions and from internal parties.

The process flow of encryption, as presented in Figure 5, includes the following steps:

- Generation of plain text bytes,
- Compression of plain text bytes,

- Generation of salt (IV),
- Concatenation of salt bytes with compressed bytes (IV || compressed plaintext),
- Generation of record key,
- Calculation of master key ($R_{key}\oplus C_{key}$),
- Encryption of concatenated bytes using AES algorithm with master key,
- Conversion of encrypted bytes to ASCII string format using Base64 encoding,
- Storing cipher text result in database as ASCII string.

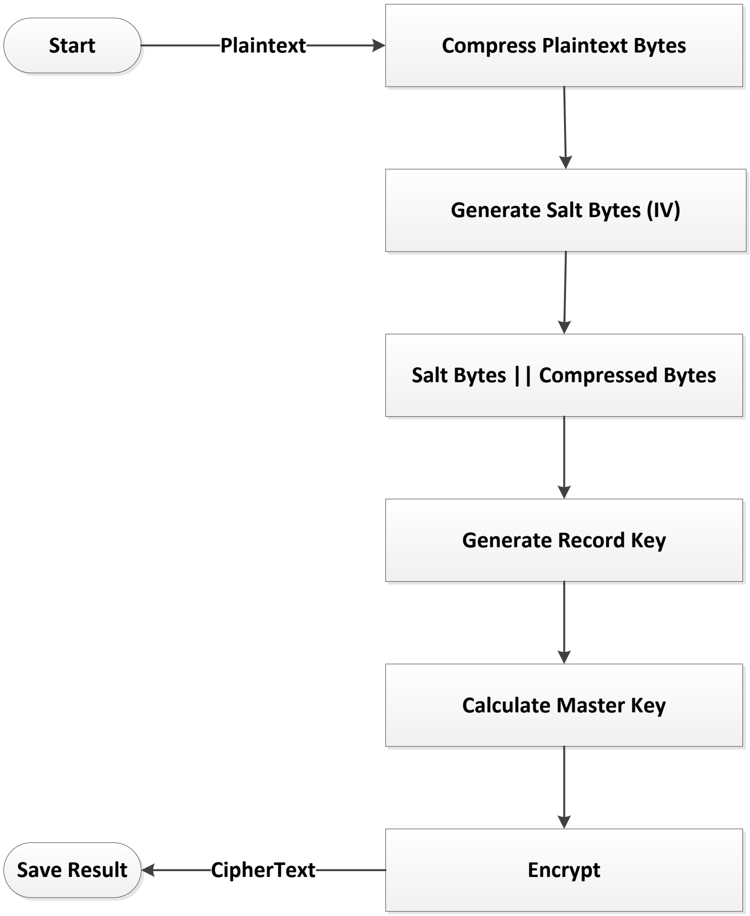


Figure 5. Encryption

Decryption

The data decryption process is provided only in client application, where the master key is derived from client and record key. During the decryption process the reverse steps of the encryption process are implemented. Figure 6 presents the decryption process, which includes the following actions:

- Removing salt from record key,
- Calculating master key ($R_{key}\oplus C_{key}$),
- Get concatenated bytes from cipher text (ASCII format string),
- Decryption of concatenated bytes (IV || compressed plaintext) with master key,
- Removing salt (IV) from compressed bytes,

- Decompressing bytes,
- Converting bytes to string,
- Display plain text result.

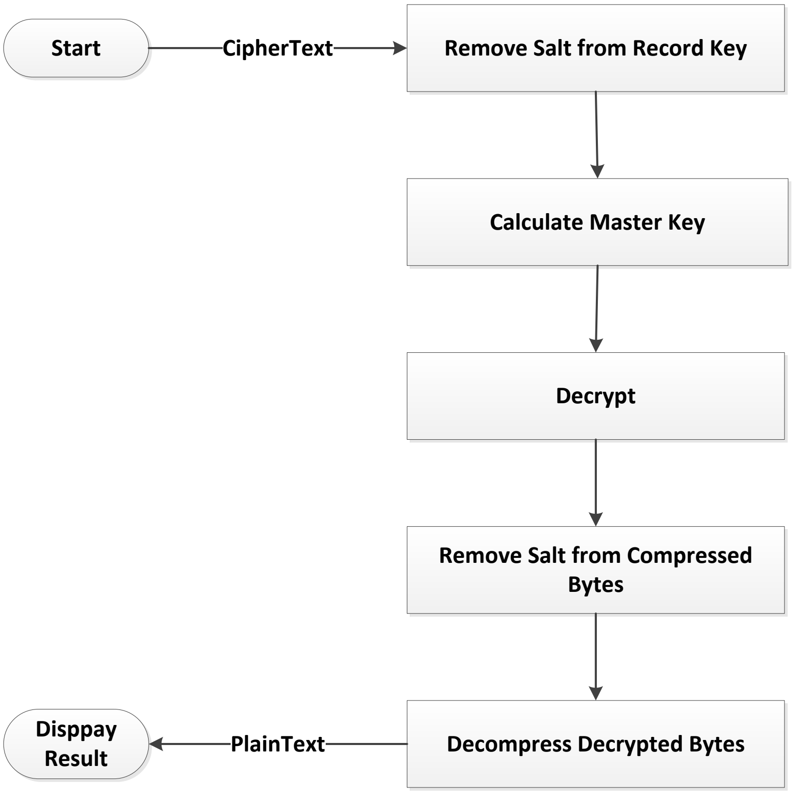

Start
CipherText
Remove Salt from Record Key
Calculate Master Key
Decrypt
Remove Salt from Compressed Bytes
Decompress Decrypted Bytes
PlainText
Disppay Result

Figure 1. Decryption

Performance

The implementation of security procedures after building systems has a direct impact on the performance and on the functionality of the system overall. Therefore, during software development we have taken in consideration the security requirement for CCMS and not only speed of encryption algorithms, as stated by (Javamex, n.d.) “it's not worth sacrificing speed for security”, as is presented in Figure 7.

According to (Harris, 2010), symmetric algorithms are much faster compared with asymmetric algorithms, and also it will be difficult to uncover encrypted data with a symmetric algorithm if a large key size is used. AES algorithm is chosen to be used for encryption/decryption due to its performance and variable key length (128, 192 and 256 bits). Based on the work of (Mattsson, 2005) AES is preferred to be used for security and for performance. An example for symmetric algorithms performance in Java is shown in Figure 7, which confirms that AES is faster even if we compare it with the Triple DES algorithm, which is well known for symmetric encryption processes. The RC4 algorithm, with different key sizes, 40 -1024 bit, is very fast, but it is of questionable security (Javamex, n.d.).

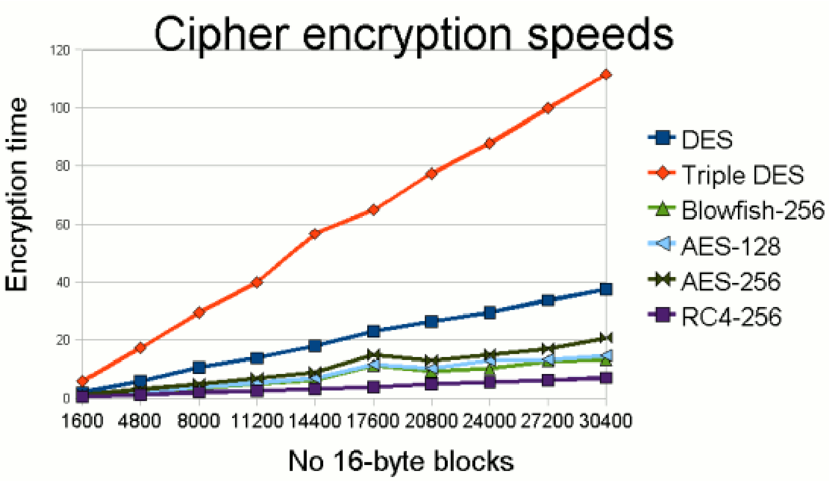


Figure 2. Performance of symmetric encryption algorithms (Javamex, n.d.).

System Architecture

Security and privacy of classified information system must be the main focus from design phase to the implementation phase. System security must be part of system architecture from the beginning. Based on the research for web application vulnerabilities (Rexha at al., 2015), conclude that security programming implementation should be raised to the highest level, maybe equal with the role of overall web application functionality. Regardless of the technology that we use to build classified information systems, web-based or windows-based applications, same security policies about data confidentiality should be implemented.

The CCMS system is an example of the implementation of security enhancement policies to record level data encryption. Managing criminal cases is the main purpose of this system, which provides registration and procession of criminal case information, violations for cases, suspects and witnesses. All this information is stored as encrypted, and in this form is transmitted from the database to client applications. In addition to criminal cases management, the system provides user management, access control, and audit of all actions. Access control can be managed according to data level, where each user can view only his cases and supervisors can view all cases of their unit or other sub-units in the hierarchy level. Audit logs are stored in a separate database, which is dedicated only for auditing.

The CCMS system consists of two applications that use SSL to exchange data over the network. The system has been implemented with three-tiered client/server architecture. Figure 8 presents the architecture of the system together with the supported infrastructure. The system components are:

- Client application – that is developed as a Windows application in C# programming language. It includes user interfaces, local data manipulation ability, and provides all communication mechanisms to enable communication with CCMS system service using SSL.
- The service of CCMS – that is developed using WCF architecture in C# programming language. WCF service handles all client requests, processes the data in the database and sends the processed result to the clients. The Windows service performs more intensive work because it is a connection point between the database and all the clients. The

advantage of using service is when we have requirement to make changes in the system. Sometimes it is enough to make changes only in the service part without the need to update the Windows application for all clients.

- Database – which runs on Microsoft SQL Server.

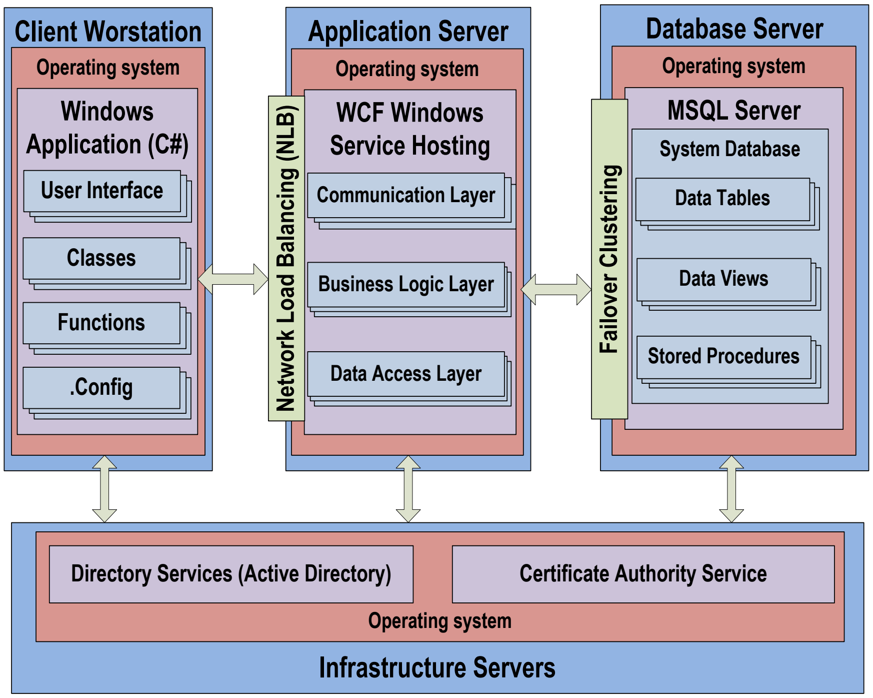
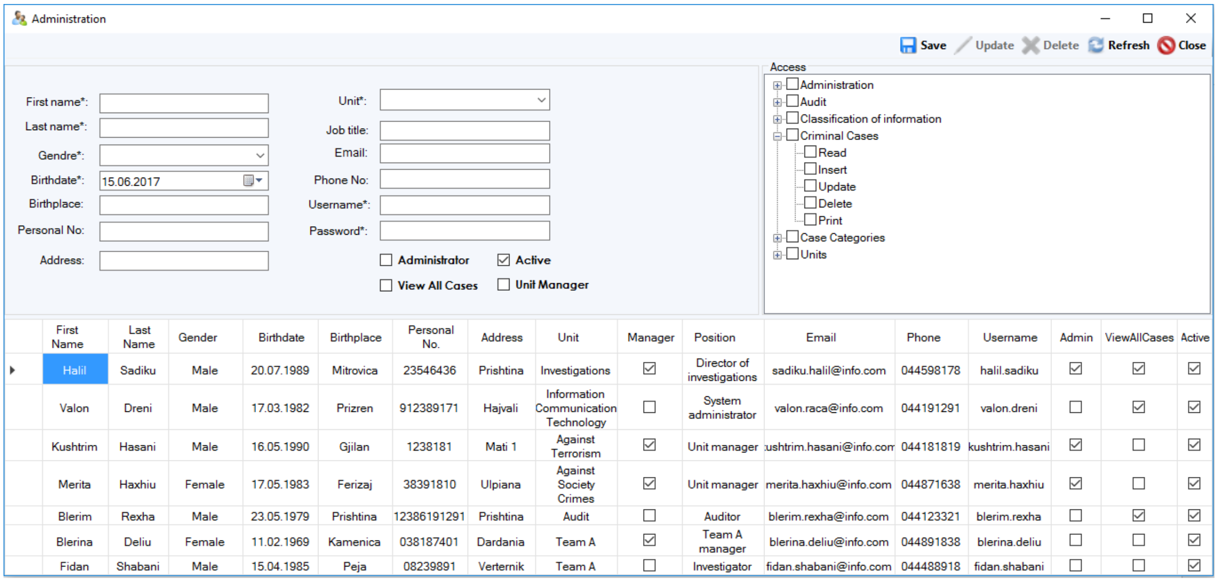


Figure 3. CCMS system architecture

Access control

Access control is the main key of information security because it is the first line that protects information from intrusions. This process enhances security of information by prohibiting unauthorized access in the CCMS system. At the same time, it does not create unnecessary barriers in the daily workflow of clients. Access control is standardized using two-factor authentication, authorization of users from administrative console, and auditing, as a supporting part of the system through which attempts for unauthorized access and other misuses are detected.

Administration console of the CCMS system provides access control and user authorizations for all components of the system. Figure 9 depicts user's administration view, such as interfaces and linked functions. For testing purposes, we have registered some users to enable the use of the system based on certain authorizations.



First name*:		Unit*:	
Last name*:		Job title:	
Gendre*:		Email:	
Birthdate*:	15.06.2017	Phone No:	
Birthplace:		Username*:	
Personal No:		Password*:	
Address:		□ Administrator	☑ Active
		□ View All Cases	□ Unit Manager

Access
- □ Administration
- □ Audit
- □ Classification of information
- □ Criminal Cases
  - □ Read
  - □ Insert
  - □ Update
  - □ Delete
  - □ Print
- □ Case Categories
- □ Units

First Name	Last Name	Gender	Birthdate	Birthplace	Personal No.	Address	Unit	Manager	Position	Email	Phone	Username	Admin	ViewAllCases	Active
Halil	Sadiku	Male	20.07.1989	Mitrovica	23546436	Prishtina	Investigations	☑	Director of investigations	sadiku.halil@info.com	044598178	halil.sadiku	☑	☑	☑
Valon	Dreni	Male	17.03.1982	Prizren	912389171	Hajvali	Information Communication Technology	□	System administrator	valon.raca@info.com	044191291	valon.dreni	□	☑	☑
Kushtrim	Hasani	Male	16.05.1990	Gjilan	1238181	Mati 1	Against Terrorism	☑	Unit manager	ushtrim.hasani@info.con	044181819	kushtrim.hasani	☑	□	☑
Merita	Haxhiu	Female	17.05.1983	Ferizaj	38391810	Ulpiana	Against Society Crimes	☑	Unit manager	merita.haxhiu@info.com	044871638	merita.haxhiu	☑	□	☑
Blerim	Rexha	Male	23.05.1979	Prishtina	12386191291	Prishtina	Audit	□	Auditor	blerim.rexha@info.com	044123321	blerim.rexha	□	☑	☑
Blerina	Deliu	Female	11.02.1969	Kamenica	038187401	Dardania	Team A	☑	Team A manager	blerina.deliu@info.com	044891838	blerina.deliu	□	□	☑
Fidan	Shabani	Male	15.04.1985	Peja	08239891	Verternik	Team A	□	Investigator	fidan.shabani@info.com	044488918	fidan.shabani	□	□	☑

Figure 4. Administration console of CCMS system

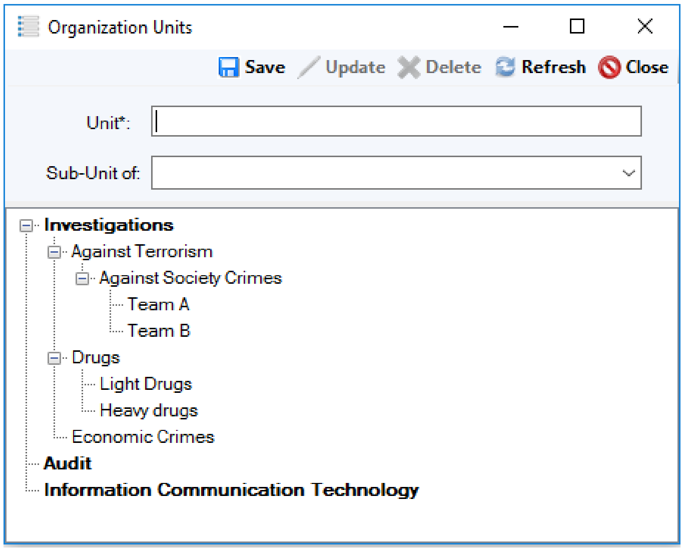
Based on the Figure 9, CCMS system provides account authorizations for two types of users:

- *Simple users* – who must be authorized for every component of system from system administrators.
- *System administrators* – who have access in all components of system. However, limitations for this type of users are made in system information. If the user is assigned as a system administrator, classified information wold not be presented to this user.

Other limitations, which are provided from access control of CCMS system are:

1. Access restrictions to the whole system:
   - Active and passive status are used to disable or re-enable an account access in the whole system without removing authorizations,
   - Not registered as user in CCMS database. Not all employees of an organisation will work with classified information systems.
2. Access restrictions for client application components, which includes authorizations for:
   - Forms,
   - Presentation of data (Read), Update, Delete and Print.
3. Restrictions on information (data) level:
   - User will view only classified information that they entered in the system,
   - Managers will view all classified information of their unit or other sub-units in the hierarchy level,
   - Explicitly view all cases for a specific user,
   - System administrators will never see classified information from the beginning where they are assigned as administrator in the CCMS system.

Restrictions on information level are managed automatically by the CCMS system in the hierarchy level of units of organization. After a user gain access read, update or delete, by default it will see only classified information that he or she enters. Managers of units can read, update or delete all classified information of workers that they manage and all of the information of sub-units. System also provides explicit privilege to view all classified information. In Figure 10 a supposed hierarchy of management units is presented. So if an investigator of "Team A" enters a criminal case, then this case can be read, updated or deleted (depending on the authorizations that management officers have in the application components) from: unit manager of "Team A", "Against the Society Crimes", "Against Terrorist", and by the senior unit manager of "Investigations".



Unit*:

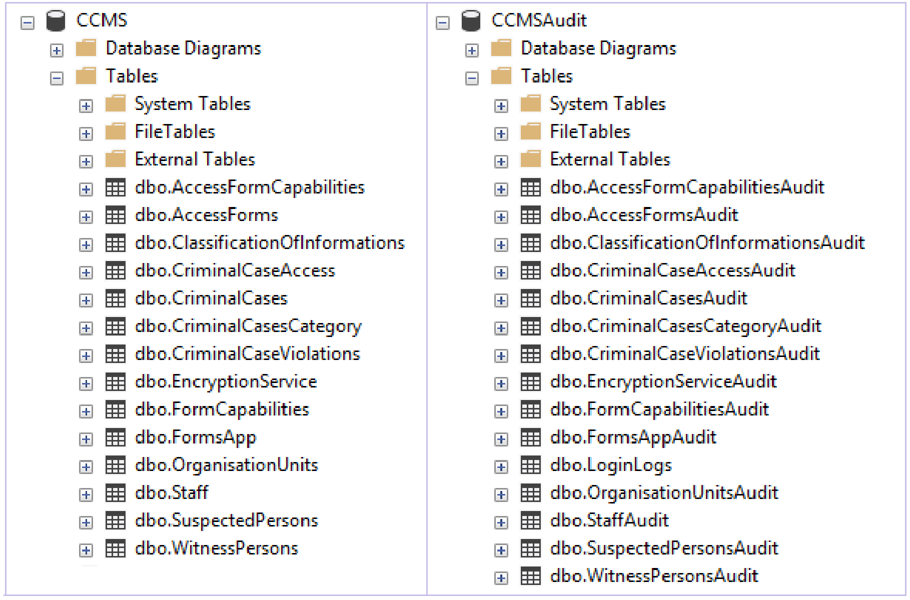
Sub-Unit of:

- **Investigations**
  - Against Terrorism
    - Against Society Crimes
      - Team A
      - Team B
  - Drugs
    - Light Drugs
    - Heavy drugs
  - Economic Crimes
- **Audit**
- **Information Communication Technology**

Figure 5. Client application - Organization Units

Audit

The most important part of each classified information system is the database. CCMS system uses two relational databases, which are presented in Figure 11.



- CCMS
  - Database Diagrams
  - Tables
    - System Tables
    - FileTables
    - External Tables
    - dbo.AccessFormCapabilities
    - dbo.AccessForms
    - dbo.ClassificationOfInformations
    - dbo.CriminalCaseAccess
    - dbo.CriminalCases
    - dbo.CriminalCasesCategory
    - dbo.CriminalCaseViolations
    - dbo.EncryptionService
    - dbo.FormCapabilities
    - dbo.FormsApp
    - dbo.OrganisationUnits
    - dbo.Staff
    - dbo.SuspectedPersons
    - dbo.WitnessPersons

- CCMSAudit
  - Database Diagrams
  - Tables
    - System Tables
    - FileTables
    - External Tables
    - dbo.AccessFormCapabilitiesAudit
    - dbo.AccessFormsAudit
    - dbo.ClassificationOfInformationsAudit
    - dbo.CriminalCaseAccessAudit
    - dbo.CriminalCasesAudit
    - dbo.CriminalCasesCategoryAudit
    - dbo.CriminalCaseViolationsAudit
    - dbo.EncryptionServiceAudit
    - dbo.FormCapabilitiesAudit
    - dbo.FormsAppAudit
    - dbo.LoginLogs
    - dbo.OrganisationUnitsAudit
    - dbo.StaffAudit
    - dbo.SuspectedPersonsAudit
    - dbo.WitnessPersonsAudit

Figure 6. CCMS system databases

Audit is a special process of the CCMS system that enables the registration and presentation of all user activities in the system. CCMS databases and their functions are:

- Transactional database is used to register classified information, which are entered by users while working with the system. Using an interface, as presented in Figure 9, the database is populated.
- Transactional database for audit is used to register all activities of users while they read, insert, update or delete data. In the audit database of the system other activities of users like login logs, print, and audited activities are also registered. Population with data will be managed only by the system as is shown in Figure 12.

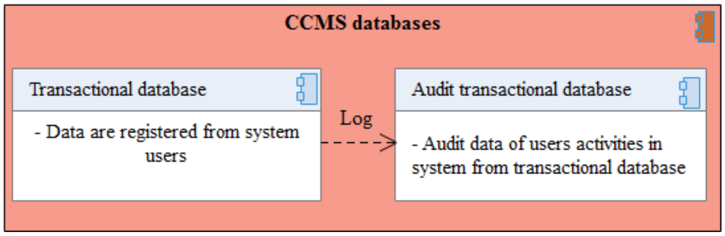
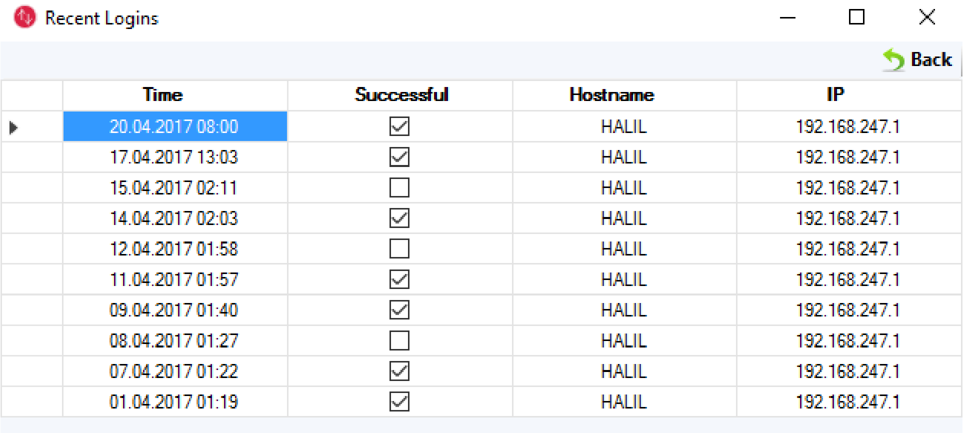

CCMS databases
Transactional database
- Data are registered from system users
Log
Audit transactional database
- Audit data of users activities in system from transactional database

Figure 7. Transactions between system databases

Audit provides the access control log for every user of the CCMS system. In Figure 13 a log form is presented, filtered by login activity, which shows the last ten attempts of a user for access to the system.



	Time	Successful	Hostname	IP
▶	20.04.2017 08:00	☑	HALIL	192.168.247.1
	17.04.2017 13:03	☑	HALIL	192.168.247.1
	15.04.2017 02:11	□	HALIL	192.168.247.1
	14.04.2017 02:03	☑	HALIL	192.168.247.1
	12.04.2017 01:58	□	HALIL	192.168.247.1
	11.04.2017 01:57	☑	HALIL	192.168.247.1
	09.04.2017 01:40	☑	HALIL	192.168.247.1
	08.04.2017 01:27	□	HALIL	192.168.247.1
	07.04.2017 01:22	☑	HALIL	192.168.247.1
	01.04.2017 01:19	☑	HALIL	192.168.247.1

Figure 8. Client application - Recent logins for a specific user

Audit process of the CCMS has created a new form that shows all activities in each component for authorized users to audit all activities in the system.

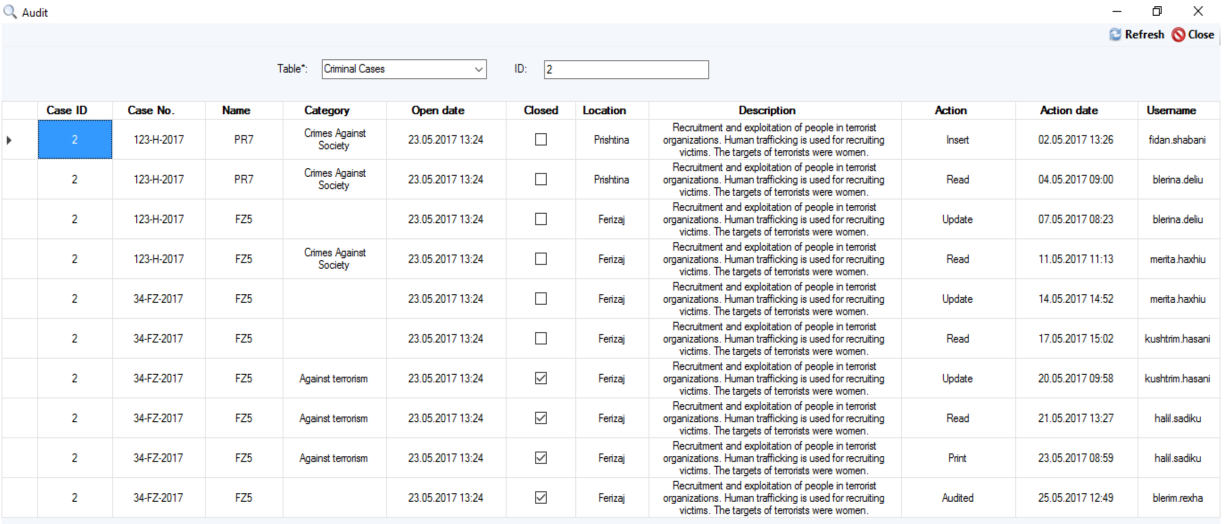


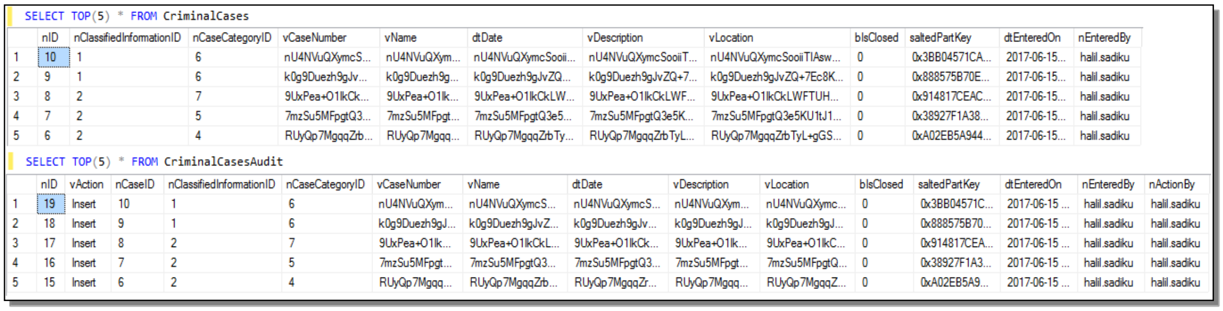
Table*: Criminal Cases

ID: 2

	Case ID	Case No.	Name	Category	Open date	Closed	Location	Description	Action	Action date	Username
▸	2	123-H-2017	PR7	Crimes Against Society	23.05.2017 13:24	□	Prishtina	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Insert	02.05.2017 13:26	fidan.shabani
	2	123-H-2017	PR7	Crimes Against Society	23.05.2017 13:24	□	Prishtina	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Read	04.05.2017 09:00	blerina.deliu
	2	123-H-2017	FZ5		23.05.2017 13:24	□	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Update	07.05.2017 08:23	blerina.deliu
	2	123-H-2017	FZ5	Crimes Against Society	23.05.2017 13:24	□	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Read	11.05.2017 11:13	merita.haxhiu
	2	34-FZ-2017	FZ5		23.05.2017 13:24	□	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Update	14.05.2017 14:52	merita.haxhiu
	2	34-FZ-2017	FZ5		23.05.2017 13:24	□	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Read	17.05.2017 15:02	kushtrim.hasani
	2	34-FZ-2017	FZ5	Against terrorism	23.05.2017 13:24	☑	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Update	20.05.2017 09:58	kushtrim.hasani
	2	34-FZ-2017	FZ5	Against terrorism	23.05.2017 13:24	☑	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Read	21.05.2017 13:27	halil.sadiku
	2	34-FZ-2017	FZ5	Against terrorism	23.05.2017 13:24	☑	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Print	23.05.2017 08:59	halil.sadiku
	2	34-FZ-2017	FZ5		23.05.2017 13:24	☑	Ferizaj	Recruitment and exploitation of people in terrorist organizations. Human trafficking is used for recruiting victims. The targets of terrorists were women.	Audited	25.05.2017 12:49	blerim.rexha

Figure 9. Client application - Auditing

Classified information is kept encrypted in both databases, and their presentation in plain text is only possible through the client application. This is presented in Figure 15, where two tables are shown, table "CriminalCases" and table "CriminalCasesAudit" containing encrypted classified information.



```
SELECT TOP(5) * FROM CriminalCases
```

	nID	nClassifiedInformationID	nCaseCategoryID	vCaseNumber	vName	dtDate	vDescription	vLocation	bIsClosed	saltedPartKey	dtEnteredOn	nEnteredBy
1	10	1	6	nU4NVuQXymcS...	nU4NVuQXym...	nU4NVuQXymcSooii...	nU4NVuQXymcSooiiT...	nU4NVuQXymcSooiiTIAsw...	0	0x3BB04571CA...	2017-06-15...	halil.sadiku
2	9	1	6	k0g9Duezh9gJv...	k0g9Duezh9g...	k0g9Duezh9gJvZQ...	k0g9Duezh9gJvZQ+7...	k0g9Duezh9gJvZQ+7Ec8K...	0	0x888575B70E...	2017-06-15...	halil.sadiku
3	8	2	7	9UxPea+O1lkCk...	9UxPea+O1lk...	9UxPea+O1lkCkLW...	9UxPea+O1lkCkLWF...	9UxPea+O1lkCkLWFTUH...	0	0x914817CEAC...	2017-06-15...	halil.sadiku
4	7	2	5	7mzSu5MFpgtQ3...	7mzSu5MFpgt...	7mzSu5MFpgtQ3e5...	7mzSu5MFpgtQ3e5K...	7mzSu5MFpgtQ3e5KU1tJ1...	0	0x38927F1A38...	2017-06-15...	halil.sadiku
5	6	2	4	RUyQp7MgqqZrb...	RUyQp7Mgqq...	RUyQp7MgqqZrbTy...	RUyQp7MgqqZrbTyL...	RUyQp7MgqqZrbTyL+gGS...	0	0xA02EB5A944...	2017-06-15...	halil.sadiku

```
SELECT TOP(5) * FROM CriminalCasesAudit
```

	nID	vAction	nCaseID	nClassifiedInformationID	nCaseCategoryID	vCaseNumber	vName	dtDate	vDescription	vLocation	bIsClosed	saltedPartKey	dtEnteredOn	nEnteredBy	nActionBy
1	19	Insert	10	1	6	nU4NVuQXym...	nU4NVuQXymcS...	nU4NVuQXymcS...	nU4NVuQXym...	nU4NVuQXymc...	0	0x3BB04571C...	2017-06-15 ...	halil.sadiku	halil.sadiku
2	18	Insert	9	1	6	k0g9Duezh9gJ...	k0g9Duezh9gJvZ...	k0g9Duezh9gJv...	k0g9Duezh9gJ...	k0g9Duezh9gJ...	0	0x888575B70...	2017-06-15 ...	halil.sadiku	halil.sadiku
3	17	Insert	8	2	7	9UxPea+O1lk...	9UxPea+O1lkCkL...	9UxPea+O1lkCk...	9UxPea+O1lk...	9UxPea+O1lkC...	0	0x914817CEA...	2017-06-15 ...	halil.sadiku	halil.sadiku
4	16	Insert	7	2	5	7mzSu5MFpgt...	7mzSu5MFpgtQ3...	7mzSu5MFpgtQ3...	7mzSu5MFpgt...	7mzSu5MFpgtQ...	0	0x38927F1A3...	2017-06-15 ...	halil.sadiku	halil.sadiku
5	15	Insert	6	2	4	RUyQp7Mgqq...	RUyQp7MgqqZrb...	RUyQp7MgqqZr...	RUyQp7Mgqq...	RUyQp7MgqqZ...	0	0xA02EB5A9...	2017-06-15 ...	halil.sadiku	halil.sadiku

Figure 10. Encrypted data stored in database

Conclusion

One of the main recommendations for all EU countries is the implementation and advancement of e-government systems. This recommendation aims to reform public administration and to increase transparency towards citizens (European Commission 2016). An inseparable part of the e-government systems is security of information and privacy, especially for government law agencies.

Classified information systems, in addition to functionality and accuracy, must meet all security requirements, as a result of the increasing trend of cyber-attacks. System performance is also an important issue that has been taken into account.

The proposed solution enhances security of information by applying cryptographic algorithms to data encryption up to record levels. A unique data flow process has been developed for all system processes ranging from authentication to auditing. Two-factor authentication is proposed to be used for all classified information systems by implementing PKI infrastructure using smart cards. Access control has been standardized in tree view. Auditing is used as an auxiliary component that prevents the misuse of classified information.

Record level encryption secures information from intrusions and from internal staff. A unique process that manages cryptography keys has been developed, which is controlled only by the system. Master key is used to encrypt and decrypt data at record level. This key is independent from all parties, it is calculated before each encryption or decryption process, and it is not stored anywhere.

In order to save storage capacities in the database, Deflate Compression Algorithm is used, which achieves 79 % savings. To make encryption of every record (row) unique, each record key and plaintext of a column are salted before encryption.

The security and privacy of information and its access are the most vital part of each classified information system. The future work that remains to be done is the implementation of session keys, which will provide a unique exchanging process, i.e. substituting SSL connection, for client keys between client application and service by using the public key of the CCMS system. While the client application is running, session key can also be used to secure (encrypt) client key on RAM memory of the client workstation.

References

Arshad, N.H. , Shah, S.N.T , Mohamed, A. , Mamat, A.M. (2007). The Design and Implementation of Database Encryption, *International Journal of Applied Mathematics and Informatics,* Vol. 1 Iss. 3, pp. 115-122.

Aarthi, G. and Ramaraj, E. (2012). A Novel Encryption approach in Database Securit, *International Journal of Computer& Organization Trends*, Vol. 2 Iss. 1, pp. 16-20.

Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S. and Kar, J. (2015) . Public Key Infrastructure: A Survey', *Journal of Information Security*, Vol.06 No. 01, pp. 31-37.

Bouganim, L. and Guo, Y. (2009). Database encryption. Encyclopedia of cryptography and security, pp. 1-9.

Department of Defense (2004) DoD Personnel Identity Protection (PIP) Program, Directive Number 1000.25.

European Commission (2015). Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information, Brussel.

European Commission (2016). EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government, Brussel. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268 (Accessed 11 January 2018)

Harris, S. (2010). Certified Information Systems Security Professional (CISSP) Exam Guide, 5th Edition.

Huey, P. (2017) Oracle Database Advanced Security Guide, *12c Release 1 (12.1)*, Oracle, E50333-16.

Josefsson, S. (2006). The Base16, Base32, and Base64 Data Encodings. RFC 4648 (Proposed Standard), http://www.ietf.org/rfc/rfc4648.txt (Accessed 2 December 2017).

Lowy, J. and Montgomery, M. (2015) Programming WCF Services: Design and Build Maintainable Service-Oriented Systems, 4th Edition.

Menezes, A. , Oorschot, P.V. and Vanstone, S. (1997). Handbook of Applied Cryptography, CRC Press, pp. 1-48.

Mattsson, Ulf T. (2005) 'Database Encryption - How to Balance Security with Performance' [online] at SSRN: https://ssrn.com/abstract=670561 or http://dx.doi.org/10.2139/ssrn.670561 (Accessed 11 December 2017)

Mahajan, A., Verma, A. and Pahuja, D. (2014) 'Smart Card: Turning Point of Technology', *International Journal of Computer Science and Mobile Computing*, Vol. 3 Iss. 10, pp. 982–987.

Microsoft. [Online] https://msdn.microsoft.com/en-us/library/system.security.cryptography.rfc2898derivebytes(v=vs.110).aspx (Accesed 25 December 2017).

Javamex. Comparison of ciphers, [Online] http://www.javamex.com/tutorials/cryptography/ciphers.shtml (Accessed on 12 December 2017).

National Security Agency, Central Security Service (2017) Information Assurance Capabilities - Data at Rest Capability Package, Version 3.8.

Oswal, S., Singh, A. and Kumari, K. (2016). Deflate Compression Algorithm, *International Journal of Engineering Research and General Science*, Vol.4 Issue 1. pp. 430-436.

Rexha, B., Lajqi, H. and Limani, M. (2010). Implementing Data Security in Student Lifecycle Management System at the University of Prishtina, *Journal Transaction on Information Science and Application*, Vol. 7 Iss. 7, pp. 965-974.

Rexha, B., Halili, A., Rrmoku, K. and Imeraj, D. (2015). Impact of secure programming on web application vulnerabilities', IEEE International Conference on Computer Graphics, Vision and Information Security, KIIT University, Bhubaneswar, Odisha, India.

Varga, S., Cherry, D., D'Antoni, J. (2016) Introducing Microsoft SQL Server 2016: Mission-Critical Applications, Deeper Insights, Hyperscale Cloud, Microsoft Press, Redmond, Washington.