SECURITY OF CRITICAL DATA IN DATABASE – AN OVERVIEW

*Naulesh Kumar

ABSTRACT

Today, it is imperative for enterprises to know which specific threats they are trying to protect against and take stringent measures to address those threats. A networks to bring complete data privacy to the enterprise has been proposed in this paper. With this Network Data Secure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. Data Secure features a dedicated security appliance and specialized software that enables organizations to encrypt data in applications and databases. Using the proposed technique organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. The administrators are encouraged to focus on developing key management and administrative policies for their organizations that will provide maximum security.

Keywords: *Database, Network Data Security, Encrypt, Security*

1. INTRODUCTION

In the current scenario a number of problem arises with the security of documents, files and important data. So, there is a need to have a technique to protect the documents which avoids the unauthorized access of data in an unsecure communication environment.

There are various techniques which are used to keep the data confidential from hackers. Some of these are passwords, cryptography and biometrics. Passwords are not so good for this task due to their low entropy. Biometrics technique produces harmful effects on the human beings and it is too costly. Due to these above problems cryptography is the best solution for security. A plaintext is a message to be communicated in a secret way. Encryption is the process of creating a cipher text (hidden data) from a plaintext and decryption is the reverse process of encryption, where cipher text is converted into plaintext. The study of encryption and decryption is called cryptology and cryptography is the application of them. For encode, a plaintext changes the plaintext into a series of bits or numbers alpha-numeric may be used which include A to Z and 0 to 9 values. The most common method of encoding a message these days is to replace it with its ASCII value, which is an 8 bit representation for each symbol. The process of decoding turns bits or numbers back into plaintext, is called decryption. Cryptography is the best method to protect data and Important files from unauthorized parties. It is the science of writing the data in secret code and about the design and analysis of mathematical techniques that enables secure communication in the presence of millions adversaries.

*Vidya Memorial Institute Of Technology, Tupudana, Ranchi, Jharkhand

2. OBJECTIVES

For achieving the data security, encryption is the most effective way everywhere and everyplace where security is needed. The process of hiding the contents of a message in such a way that the original information is recovered only through a decryption process is called encryption. The purpose of Encryption is to prevent unauthorized parties from viewing crucial information. An encryption occurs when the data is passed through some substitute technique like shifting technique, table references or mathematical operations. A different form of data is generated through these processes. The unencrypted data is called plaintext and the encrypted data is called cipher text. This represents the original data in a different form. Encryption key is used to encrypt the original message which depends upon key based algorithms.

There are two general categories for key based Encryption algorithm first one is called Symmetric Encryption (SE) which uses a single key to encrypt the message and decrypt the message. Second is Asymmetric Encryption (AE) which uses two different keys a public key to encrypt the message, and a private key to decrypt the message. There are several different types of key based Encryption algorithms such as DES, RSA, PGP, Elliptic curve but all of these algorithms depend on high mathematical manipulations.

3. RESEARCH METHODOLOGY

3.1 Database Integration Process

As the incidence and severity of security breaches continues to grow, it is increasingly incumbent upon organizations to begin encrypting data inside the enterprise. KUMARNET offers breakthrough solutions that make it practical to encrypt critical data, and ensure it's secured throughout an organization. With this Data Secure Platforms, organizations can better ensure that they are compliant with legislative and policy mandates for security, and eliminate the risks of a breach. KUMARNET Data Secure Platforms deliver comprehensive security capabilities:

- Encrypt critical data in Web servers, application servers, and databases.
- Ensure all access to critical data is carefully managed, logged, and controlled.
- Administer keys and policies in a secure, centralized fashion.
- Ensure security processing is highly scalable and reliable.

Data Secure encrypts data in the database at the column level, and can be used to secure such information as credit card numbers, social security numbers, passwords, account balances, and email addresses. Data Secure significantly streamlines the administrative tasks involved in database encryption—it automates much of the configuration and implementation process and it can be deployed without any disruption to the applications tied to the database. The KUMARNET Data Secure Platform is comprised of three components:

- The Data Secure appliance, a dedicated hardware system,
- The Network-Attached Encryption (NAE) Server, which runs on the Data Secure appliance.
- The KUMARNET NAE Connector, software that is installed on the Web, application, or database server.

The NAE Connector features standards-based cryptographic interfaces that allow the protection of user-defined data through integration of security functions at the business logic layer. These small software components are installed on each database that has a need to interface with the Ingrian appliance, and they initiate encrypt and decrypt operations.

4. ANALYSIS AND INTERPRETATION

4.1 How it Works

Integrating the Data Secure platform in your existing database infrastructure is a straightforward, automated process. The NAE Connector component outlined above consists of a complete code to manage a seamless interaction between the database and the Data Secure platform. The Data Secure appliance features a secure, Web-based user interface that walks administrators through a step-by-step configuration process and, once parameters have been set, even automates the installation of the required NAE Connector software on the database. Once installed and configured, the NAE Connector dynamically generates all the necessary stored procedures and functions to:

- Encrypt and decrypt data on demand from inside the database.
- Migrate data from plaintext to cipher text and change the database schema to accommodate encrypted columns.
- Rotate cryptographic keys.
- Automate subsequent encrypt and decrypt operations.
- Authenticate users so that only authorized users are able to access sensitive data.

This transparent integration means that you can continue using your existing SQL statements without having to modify them. And, more importantly, you do not have to write any of the logic to perform encrypt or decrypt operations from your database. Following is a high-level diagram outlining how the solution is deployed.

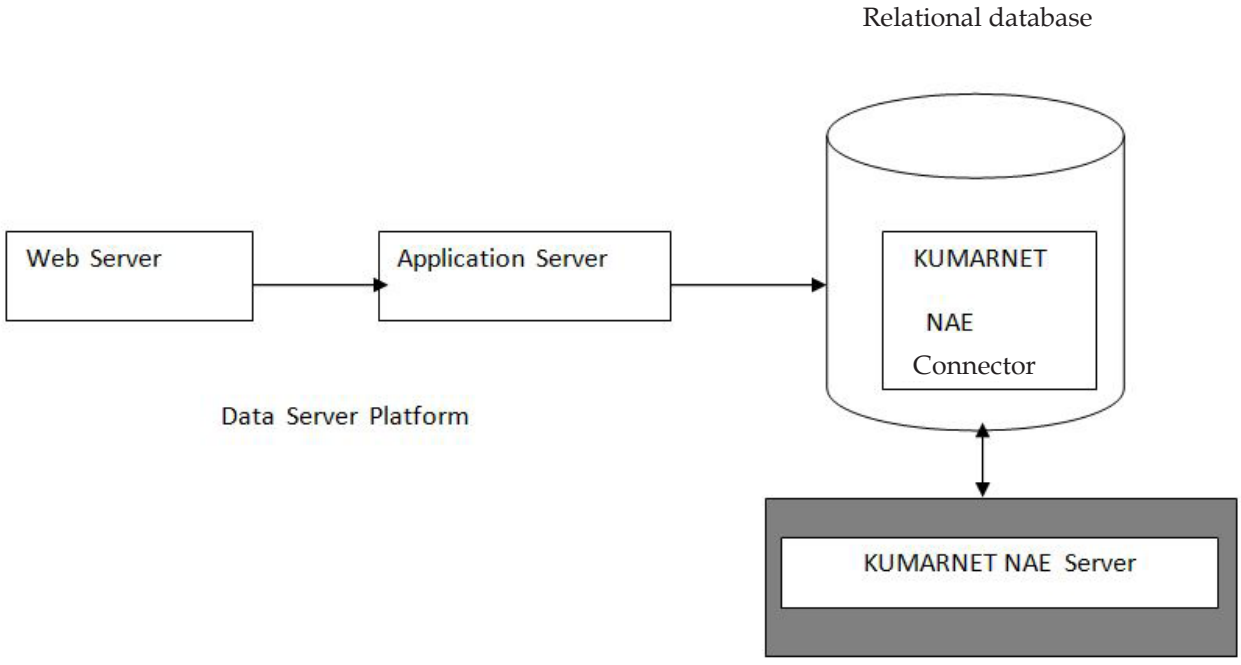

Fig 1: High Level View of Implementation with KUMARNET Data Secure Platforms

The diagram above shows a Web server accessing an application server, which is making a call to a database to access sensitive data. The NAE Connector is installed in the database and the sensitive data is stored in encrypted format within the database. The user who requests the sensitive data must have permission within the database to make a request to the NAE Connector. That user must also have access to the requested key on the NAE Server. If either of the conditions above is not met, then the user is not given access to the sensitive data. If the user is authorized to use the requested key for decryption, then the NAE Server performs the decrypt operation on the sensitive data. The decrypted data is then passed back to the database. The Data Secure appliance is the physical device where cryptographic operations and key management operations are performed. Different hardware platforms provide varying capabilities for performance and FIPS compliance. The NAE Server and all cryptographic keys reside on this hardened security system.

4.2 How Does Data Get Encrypted?

Before implementing Data Secure in your enterprise, your sensitive data is most likely to being stored as plaintext, so the logical question is: how do you migrate plaintext data into encrypted format? The process is straightforward, and, as mentioned above, KUMARNET automates this process through the Data Secure appliance's GUI. To illustrate the simplicity of the process, take social security numbers as an example. If you have a table called CUSTOMER that stores sensitive customer data like names, addresses, and social security numbers, you might want to encrypt the social security numbers. Your original CUSTOMER table might look like this:

SQL> select * from CUSTOMER;

Table 2.1. Sensitive Data Is Stored In the Column SSN.

NAME	SSN	ADDRESS	CITY	STATE	ZIP
Ranjan	123456789	Ranchi	Ranchi	Jharkhand	835220
Nitin Mohan	ABC246809	Delhi	Delhi	Uttar Pradesh	110030
N.Kumar	BIT1018-04	Belly Rd.	Patna	Bihar	800001
Raj kiran	HCL04CS16	Kakinara	Andhra	Andhra	630032

The first step in the process of securing your sensitive data is to identify what data you want to secure and where that data resides. In this example, social security numbers are stored in a column called SSN. Once you have identified the sensitive data, you can configure KUMARNET to automate this data protection process. During the first step, KUMARNET renames the table in which the sensitive data resides; the table must be renamed so that a view can be created later with the same name as the original table.

In the next step, KUMARNET creates a temporary table and exports the sensitive data to that temporary table. Notice in Figure 4 below that SSN is the only column exported to the temporary table from the original table. The Row_ID column is added automatically and used later when returning the encrypted data back to the original table. The values in the column that held the sensitive data in the CUSTOMER_ENC table (remember—the CUSTOMER table was renamed) are set to null to avoid any data conversion issues that might arise when changing the data type in a later step.

Before Ingrian can populate the original column with encrypted data, it must modify the column size and data type because encrypted data is predictably larger than plaintext data, and most likely, your social security numbers are stored as some sort of integer or character data type. Although KUMARNET gives you the option to store your encrypted data in Base64 encoded format, it is recommended that you store your encrypted data in binary (the default choice during configuration) because binary data is smaller than Base64 encoded data and there is less overhead with binary because the system does not have to encode and decode data with every encrypt or decrypt operation.

Once the column is modified, KUMARNET can migrate the sensitive data back into the CUSTOMER_ENC table. Before the data is imported back into the CUSTOMER_ENC table, however, the NAE Connector sends the data to the NAE Server, where the data is encrypted. The NAE Server returns the encrypted data to the NAE Connector, which then inserts the encrypted data into the CUSTOMER_ENC table.

SQL> select *from CUSTOMER_ENC;

NAME	SSN	ADDRESS	CITY	STATE	ZIP
Ranjan	[B@ 388993	Ranch	Ranchi	Jharkhand	835220
NitinMohan	[B@ b8f82d	Delhi	Delhi	Uttar Pradesh	110030
N.Kumar	[B@ 1d04653	Belly Rd.	Patna	Bihar	800001
Rajkiran	[B@b8f82d	kakinara	Andhra	Andhra	630032

4.3 How Do You Automate Subsequent Updates and Inserts?

Once your table and column are able to accommodate encrypted data, KUMARNET automates encryption and decryption of data by creating a view, triggers, and stored procedures that are generated during configuration to work with the NAE Connector. In this way, properly authenticated applications outside the database can continue to query and update the same database tables as before. The NAE Connector remains transparent to outside applications, and, more importantly, the amount of code changes necessary to integrate the NAE Connector is minimal. When sensitive data is accessed, the view is instantiated by the database and populated with decrypted data from the CUSTOMER_ENC table. Because the view has the same name as the original table, all SQL statements that reference the encrypted data can function regularly without modification. Likewise, triggers trap all the inserts and updates executed on the view. If an insert statement is detected, a new insert statement is generated based on the original insert values. The social security number in this case is encrypted before insertion into the base table. Similarly, when an update statement is executed, a new update statement is generated to update the base table.

As it is mentioned above, the process to migrate plaintext data to encrypted format is quite simple when using the NAE Connector; furthermore the process can be completely automated through the use of triggers, views, and stored procedures, all of which are created and Installed by the Data Secure appliance during configuration. What's most important is that the integration is completely transparent to applications that interface with your sensitive data. Before deploying Data Secure, your sensitive data sits in the clear in your databases. After deploying Data Secure, your sensitive data is encrypted, and applications can continue interacting with sensitive data using the same SQL statements; however, instead of interacting directly with that sensitive data, the application servers are actually interacting with a view of the data in Relational Database.

4.4 Output of Java Program

Output of the java program is shown below in Command Prompt.

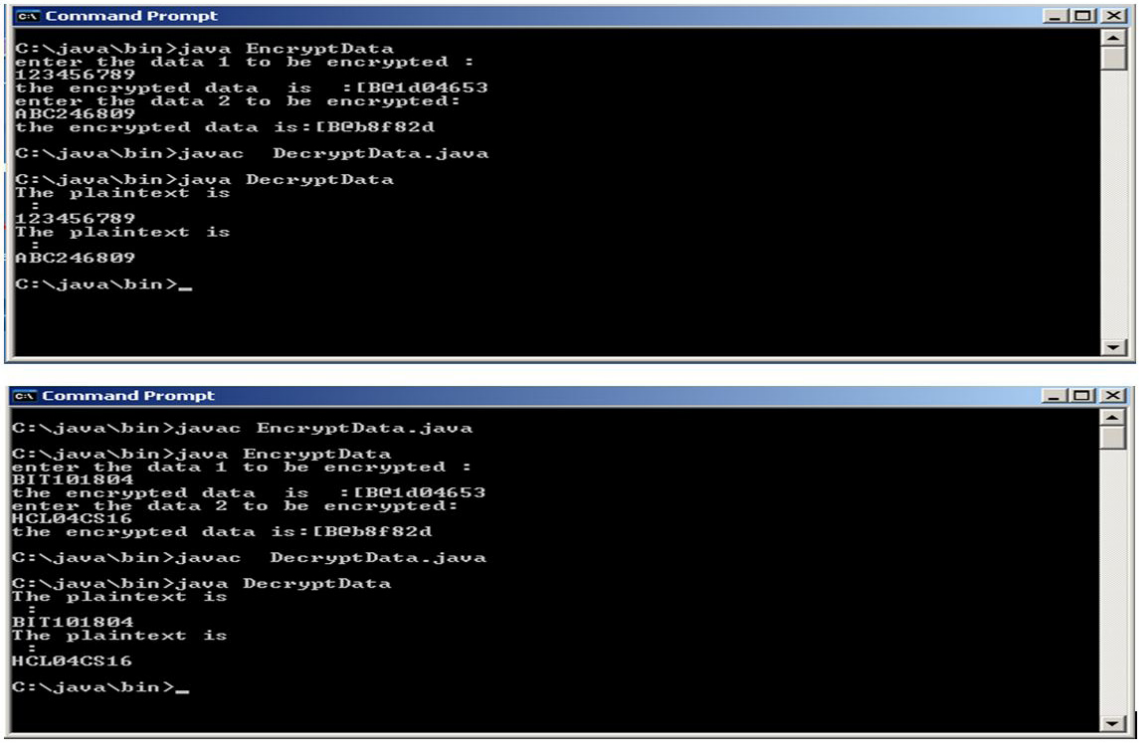

Fig 2: Output of the data (SSN) in Encrypted and Decrypted form.

5. APPLICATIONS AND FUTURE WORK

Cryptography is utilized in various applications and environments. The specific utilization of encryption and the implementation of TDEA will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft or technical intrusion (e.g., hacker attacks). In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period. This Network brings complete data privacy to the enterprise. Data Secure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases.

REFERENCES

1. *Fundamentals of Network Security, Eric Maiwald, Dreamtech publication*
2. *Cryptography and Network Security Principle and Practice, Stalling William*
3. *Data Communications and Networking, Behrouz A. Forouzans.*
4. *Starting Out with Oracle covering Database, John Day Craig,Van Slyke*
5. *Internet & JAVA Programming, R.Krishnamoorthy, S.Prabhu*

Internet Resources.

1. http://ieee.org
2. http://csrc.nist.gov/encryption/aes