Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 83 (2015) 33023-33025

ISSN: 2229-712X

Data Security using Encryption Technique

Pareek Sarthak
Anand International College of Engineering Jaipur, Rajasthan, India.

ARTICLE INFO

Article history:
Received: 18 April 2015;
Received in revised form:
26 May 2015;
Accepted: 5 June 2015;

Keywords
Database,
Security,
Encryption,
Access Control,
cryptography,
Floating point number.

ABSTRACT
Problem faced by today's communicators is not only security but also the speed of communication and size of content. Security in today's world is one of the important challenges that people are facing all over the world in every aspect of their lives. In this paper a method is proposed in which the concept of compression and data encryption is used. In this first data is compressed to reduce the size of the data and increase the data transfer rate. Thereafter compress data is encrypted to provide security.

Introduction

While information security plays an important role in protecting the data and assets of an organization, we often hear news about security incidents, such as defacement of websites, server hacking and data leakage. Organizations need to be fully aware of the need to devote more resources to the protection of information assets, and information security must become a top concern in both government and business. The present network scenario demands exchange of information with more security and reduction in both the space requirement for data storage and the time for data transmission. This can be accomplished by compression and encryption, such kind of system is called compression–crypto system. Encryption is indeed a secure coding technique and data compression is also a coding technique, whose purpose is to reduce both the space requirements for data storage and the time for data transmission. In proposed system i.e. data security using private key encryption system encoded string is produced by a model from an input string of symbols and based on arithmetic coding that can be used to achieve the present network scenario for exchange of information with more security and compression.

Data Compression

Data compression is an approach for reducing communication costs by using available bandwidth effectively. It reduces the redundancy in data representation to decrease the storage required for that data. Over the last decade there has been an unprecedented explosion in the amount of digital data transmitted via the Internet, representing text, images, video, sound, computer programs, etc. In the more modern model-based paradigm for coding, where, from an input string of symbols and a model, an encoded string is produced that is a compressed version of the input. The decoder, which must have access to the same model, regenerates the exact input string from the encoded string .The model, is a way of calculating, in any given context, the distribution of probabilities for the next input symbol. It must be possible for the decoder to produce exactly the same probability distribution in the same context. Compression is achieved by transmitting the more probable symbols in fewer bits than the less probable ones. More complex models can provide more accurate probabilistic predictions and hence achieve greater compression. The effectiveness of any model can be measured by the entropy of the message with respect to it, usually expressed in bits/symbol. Shannon's fundamental theorem of coding states that, given messages randomly generated from a model, it is impossible to encode them into less bits (on average) than the entropy of that model. A message can be coded with respect to a model using either Huffman or arithmetic coding. It's well known that the Huffman's algorithm generates minimum redundancy codes compared to other algorithms. But the disadvantage of Huffman is that, all codes of the encoded data are of different sizes. Therefore it is very difficult for the decoder to know that it has reached the last bit of a code. Arithmetic coding can be viewed as a generalization of Huffman coding. It efficiently represents more frequently occurring sequences of pixels values with fewer bits. Arithmetic coding typically has a better compression ratio than Huffman coding, as it produces a single symbol rather than several separate code word and can be used in compression based encryption system.

Cryptography

The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction. Cryptography is used to solve the above issues. It is the foundation of all information security aspects. The techniques employed to this end have become increasingly mathematical of nature. Classical cryptosystems is very easy to understand, easily implemented and very easy to be broken and because of that reason new forms of cryptography came after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium. In the last few decades, however, the trend has been on placing cryptography

Tele:
E-mail addresses: sarthakpareek1710@gmail.com

onto a sound mathematical framework. This modern focus has initiated the evolution of the field from an art into a science, which includes just about any network, particularly the internet. This evolution comes with modern cryptography (MC) really begins with Claude Shannon arguably the father of mathematical cryptography. Today's cryptographic techniques have become the immediate solution to protect information against third parties. These techniques required that data and information should be encrypted with some sort of mathematical algorithm where only the party that shares the information could possible decrypt to use the information

There are two types of cryptographic schemes: symmetric (private key) cryptography, and asymmetric cryptography, each of which described below.

Symmetric Key Cryptography

In symmetric key cryptography (also known as private-key cryptography), a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone, you have never met; you will need to figure out a way to exchange keys in a secure way. One method is to send it via another secure channel.

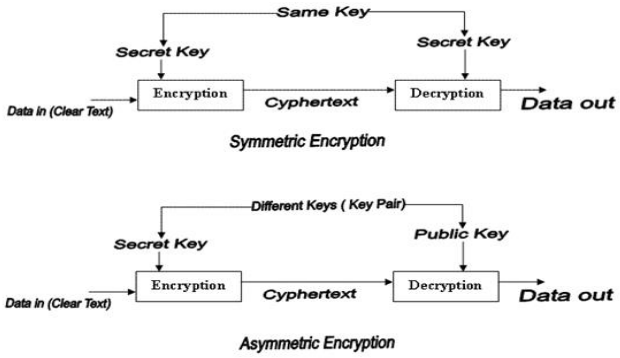

Figure 1. Symmetric and Asymmetric Encryption

Asymmetric Key Cryptography:

In the two-key system, (also known as the public key system) one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message.

Encryption

Encryption is the process of concealing or transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. The resulting encoded information is called as encrypted information. Data is valuable assets of an organization. So its security is always a big challenge for an organization. In recent times security of shared databases was studied through cryptographic viewpoint. Different governmental, non-governmental, and private and many other organizations have sensitive data on web servers that really need to be protected from attacker. To make the databases secure different security techniques were developed. One of them is encryption techniques. Though encryption improves the protection but its implementation decisions are also very important. Developing the encryption strategies arises some important questions also, like how, when and where the encryption will be performed. Encryption algorithm, symmetric or asymmetric is not explained in this framework. The encryption algorithms affect the performance of query processing and security analysis badly. Other important research issues related to this framework: first, the best encryption algorithm used in the mixed cryptography database on performance and security perspectives; second, access control methods used to control access for all parities using the database; and finally indexing and joining between different databases. It does not matter which access control method is used; there are no of ways to avoid the authorization imposed by the database server. For instance, the information system can be intruded by stalker who tries to source the database impression on disk. Databases are being outsourced to database service providers (DSP) that also welcomes the threats. The database owner has no other choice than to trust the DSP's. Than the database administrator can also miss use his rights and spay the database. Three encryption levels are defined. Storage-level encryption, database-level encryption and application-level encryption. Storage level encryption encrypts the data in the storage subsystem. It is transparent thus avoids the risk of any change in existing application.

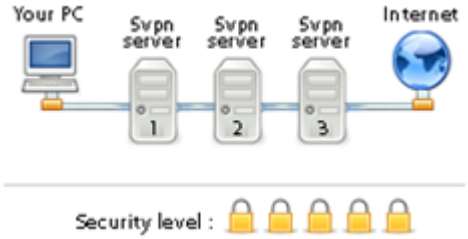

Figure 2. Three Levels where Encryption is performed

Encryption is defined as encoded information that is only readable and decoded by the persons whom the information is intended. This study discusses how the Transparent Data Encryption technology is utilized to secure against data frauds and theft. The basic technological meaning of Transparent Data encryption is encoding or encrypting databases on networks, hard disk and/or on any backup media to provide highly configurable, transparent, safe and secure environments for application development. Microsoft SQL Server 2008 uses this technology to encrypt database content stored on any network, disk or backup medium along with process of creation of a Master Key. This involves creation of key, protection by the certificate and ways to set the database to use in Microsoft SQL Server 2008 encryption. This study investigates what Microsoft SLQ Server 2008's configurable environment has to offer in terms of data safety, security and application development for developers. A new light weight encryption method is proposed that is used for columns stored in data ware houses with trusted servers. The new method is called Fats Comparison Encryption (FCE). Its overhead makes the comparison fats and efficient. So far we have discussed the work done on database security using Encryption. Now the next section will present the comparison of the study done so far.

Conclusion & Future scope

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database is vulnerable to hosts of attacks.

The proposed technique provides an excellent integration of data compression with the cryptography to increases the data security and transfer rate during data communication. In this technique we can reduce the size of data using the arithmetic encoding data compression technique and after that compressed data can be encrypted to provide the security. The Present network scenario demands exchange of information with reduction in both space requirement for data storage and time for data transmission along with security. This technique fulfils all such requirements as this technique use the concept of data compression and encryption. In this study major security issues faced databases are identified and some encryption methods are discussed that can help to reduce the attacks risks and protect the sensitive data. It has been concluded that encryption provides confidentiality but give no assurance of integrity unless we use some digital signature or Hash function. Using strong encryption algorithms reduces the performance. The future work could be carried out make encryption more effective and efficient.

References

• SHANNON C. E, (1948). "A Mathematical Theory of Communication". The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656

• Jagdish H.Pujar & Lohit M.Kadlaskar "A new lossless method of image compression and decompression using Huffman coding technique" Journal of Theoretical and Applied Information Technology.

• Mamta Sharma, (2010) "Compression Using Huffman Coding" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

• Glen G. Langdon, (1984) "An introduction to arithmetic coding", IBM Journal of Research and Development Volume 28, No.2

• Whitfield Diffie & Martin E. Hellman,(1979) "Privacy and Authentication: An Introduction to Cryptography proceedings of the IEEE, vol.67, no.3

• Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz "Hybrid Compression Encryption Technique for Securing SMS", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)

• Deo Brat Ojha, Ajay Sharma, Abhishek Dwivedi, Nitin Pande,& Amit Kumar(2010) "Space-Age Approach To Transmit Medical Image With Code Base Cryptosystem Over Noisy Channel," published in International Journal of Engineering Science and Technology Vol. 2(12),7112-7117.