ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Web Database Security Algorithms

Sweety R. Lodha[1]
Dept. of Computer Science and Engineering
Sipna College of Engg. and Technology
Amravati, Maharashtra, India

S. Dhande[2]
Assistant Professor
Dept. of Computer Science and Engg.
Sipna College of Engg. and Technology
Amravati, Maharashtra, India

Abstract: ***Databases that preserve past records of activities and data offer the important benefit of system accountability. Past events can be analyzed to detect violation and maintain data quality. System designers need to carefully balance the necessity for privacy and responsibility by controlling how and when data is held by the system and who will be able to recover and analyze it. As organizations increase their dependency on, possibly distributed, information systems for daily business, they become more vulnerable to security violation even as they increase productivity and efficiency advantages. Though a number of techniques, such as encryption and electronic signatures, are currently available for the protection of data when transmitted across sites. In this paper we present an encryption scheme that solves security problem at some level. Steganography and Cryptography are two popular ways of sending very important information in a secret way. One hides the existence of the message and the other alters the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In steganography also we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message.***

I. INTRODUCTION

Errors and malicious behavior can never be perfectly avoided; most of the applications that manage sensitive data preserve a historical record of different activities and data. This provides responsibility because past events can be analyzed to detect violations, maintain data quality, and audit compliance with security policies. For example, when managing medical information, accountability is vital. If false information is found out in a patient's medical record, it is important to find out who is responsible for the error, when it occurred. As organizations increase their adoption of database systems as the key data management technology for day-to-day operations, the security of data managed by these systems becomes vital. Damage and exploitation of data affect not only a single user or application, but may have terrible effects on the entire organization.

A complete solution to data security must meet the following three requirements: 1. privacy or confidentiality refers to the protection of data against illegal disclosure, 2. integrity refers to the avoidance of illegal and improper data alteration, and 3. availability refers to the prevention and recovery from hardware and software bugs and from malicious data access rejections making the database system unavailable.

In encryption there is the problem in which one party (Alice) having its own database and wants to outsource it to a second party (Bob), even though the trust of Alice in Bob is partial? Alice wants to be confident that the data she outsources is depicted neither to another party nor to Bob. Authorized options, such as contracts, are available, but their efficiency is often limited [1]. Here, Alice would like to have the data encrypted and only provide the ciphertext i.e. data in unreadable form to Bob, the database service provider. But if Bob is not trusted person, he cannot participate in the encryption/decryption process which is used for transmitting data securely. Usually Bob does not just store the data, but also processes non-trivial doubts sent by Alice and therefore should be able to process these doubts without decrypting the stored data.

Cryptography [2] and Steganography [2] are popular and widely used techniques that manipulate information (messages or data) in order to cipher or hide their existence from attacker respectively. Steganography is the art and science of communicating in a way which hides the existence of data used in the communication. Cryptography scrambles a message so it cannot be understood by attacker; the Steganography hides the message so it cannot be seen. Presently we have very secure methods for both cryptography and Steganography – AES algorithm is one of the secure techniques for cryptography and the Steganography methods, which use frequency domain, are highly secured. Even if we combine these both technique straight forwardly, there is a chance that the intruder may notice the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding.

II. Related Work

Early research efforts in the area of access control and confidentiality for DBMSs focused on the development of two different classes of models, based on the unrestricted access control policy and on the mandatory access control policy. This early research was transmitting in the framework of relational database systems. The relational data model, being a declarative and high-level model for specifying the logical structure of data, made the development of simple declarative languages for specifying access control policies. These earlier models and the unrestricted models in particular, introduced some important principles [3] that set apart access control models for database systems from access control models adopted by operating systems and file systems. The primary principle was that access control models for databases should be expressed in terms of the logical data model; thus authorizations for a relational database should be expressed in terms of relations i.e. in tabular form, relation attributes, and tuples. The next principle is that for databases, in addition to name-based access control, where the protected objects are specified by specifying their names, content-based access control has to be supported. Content based access control permits the system to decide whether to provide or deny access to a data item based on the contents of the data item. The development of content based access control models, which are, in general, based on the requirement of conditions against data contents, was made easy in relational databases by the availability of declarative query languages, such as SQL. In the area of unrestricted access control models for relational database systems, an important early contribution was the development of the System R access control model [4], [5], which strongly manipulated access control models of current commercial relational DBMSs. Some key features of this model included the notion of distributed authorization administration, dynamic grant and revoke command of authorizations, and the use of views for supporting content-based authorizations. Also, the initial format of familiar commands for grant and revoke of authorizations that are today part of the SQL standard. Next research proposals have extended this basic model with a variety of features, such as negative authorization,[6] role-based and task based authorization[7], [8], temporal authorization[9], and context-aware authorization. This weakness makes unrestricted access controls vulnerable to malicious attacks, such as Trojan horses embedded in application programs. A Trojan horse is a program with an apparent or actually very useful function, which contains some hidden functions exploiting the genuine authorizations of the invoking process. Sophisticated Trojan horses may leak information by means of covert channels, enabling unauthorized access to data. A covert channel is a component or feature of the system that is misused to encode or represent information for illegal transmission, without breaching the stated access control policy. A large variety of components or features can be misused to create covert channels, including the system clock, operating system inter process communication primitives, error messages, the existence of specific file names, the concurrency control mechanism, and so on. The area of compulsory access control and multilevel database systems tried to address such problems through the development of access control models based on information classification, some of which were also incorporated in commercial products. Early compulsory access control models were mainly developed for military applications and were very inflexible and suited, at best, for closed and controlled environments. There was considerable debate among security researchers concerning how to eliminate covert channels while managing the essential properties of the relational model. In particular, the concept of poly instantiation, that is, the presence of multiple copies with different security levels of the same tuple in a relation, was developed and articulated in this period [10]. Because of the lack of applications and commercial success, companies developing multilevel

DBMSs discontinued their production several years ago. Covert channels were also widely examined with considerable focus on the concurrency control mechanisms that, by matching transactions running at different security levels, would introduce an obvious covert channel. However, solutions developed in the research arena to the covert channel problem were not incorporated into commercial products.

This section present a review on some of the most recent and related work. But, before we proceed, let us describe the basic components and approaches of steganography. A steganography system usually consists of three key components, named as, secret, cover media, and stego media [11]. For a secure steganography system, four components are required, which is the key or the password. In general, the secret and the cover media can have the form of text, video, image, audio file or other media file as well. For the steganography approaches, there are four basic approaches that can be used to achieve steganography; these are as follows [12]:

- Lease Significant Bit (LSB) approach: In the LSB approach, the LSB of each byte of the cover file is replaced with bits from the message.
- Injection approach: In the injection approach, the source message is hidden in sections of the cover file that are ignored by the processing application. Therefore, avoid modifying those file bits that are related to an end-user leaving the cover file perfectly usable.
- Substitution approach: In the substitution approach, the least significant meaningful content of the cover file is replaced with the source message in a way that causes the least amount of distortion to the cover file.
- Generation approach: It is different from injection and substitution; it does not require an existing cover file but generates a cover file for the sole purpose of hiding the message.

A large number of steganography algorithms have been developed utilizing the above all the four approaches.

III. Different Algorithm Used for Web Database Security

Different algorithms are used for web security which is mentioned in this paper. One of them is encryption algorithm. Encryption is divided into three different levels. Storage-level encryption amounts to encrypt data in the storage subsystem and thus protects the data at rest. It is well suitable for encrypting files or entire directories in an operating system context. From a database point of view, storage-level encryption has the advantage to be transparent, thus avoiding any changes to existing applications. On the other side, the storage subsystem has no knowledge of database objects and structure; the encryption strategy neither to be related with user privileges, nor to data sensitivity. Database-level encryption allows securing the data as it is inserted or entered to, or retrieved from the database. The encryption strategy can be the part of the database design and can be related with data sensitivity and/or user privileges. Selective encryption is possible and can be done at various granularities, such as relations, attributes, and tuples. It can even be related with some logical conditions. Depending on the level of combination of the encryption feature and the DBMS, the encryption process may incur some modification to applications. Application-level encryption moves the encryption/decryption process to the applications that generate the data. Encryption is thus performed within the application that initiates the data into the system; the data is sent encrypted, thus naturally stored and retrieved encrypted data [13], to be finally decrypted within the application. This approach has the benefit to separate encryption keys from the encrypted data stored in the database since the keys never need to leave at the application side. The three strategies described above are pictured in following figure:

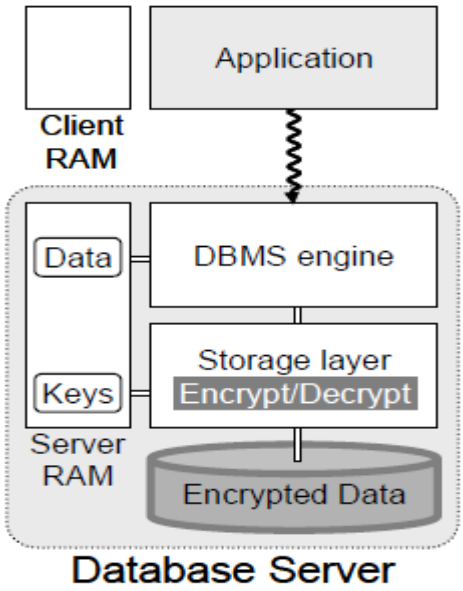

Fig. 1 Storage-level Encryption

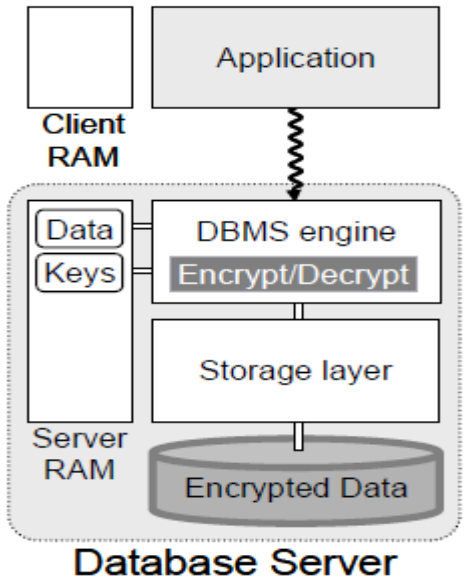

Fig. 2 Database-level Encryption

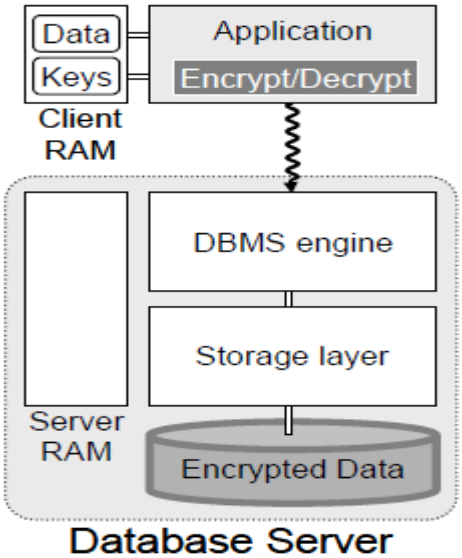

Fig. 3 Application-level Encryption

Other algorithms which are used for transmitting the data securely on web are the cryptography and steganography. There are many aspects to security and many applications. One essential aspect for secure communications is the cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself enough. There are some specific security requirements [14] for cryptography, including authentication, privacy /confidentiality, and integrity non-repudiation. The three types of algorithms are described:

- Secret Key Cryptography (SKC): Uses only one key for both encryption and decryption.
- Public Key Cryptography (PKC): Uses two different keys, one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly encrypt information.

Steganography is another technique for secured communication. It encompasses methods of transmitting secret messages through safe cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in audio, text, images [15], video, or some other digitally representative code. Steganography systems can be grouped by the type of covers [16] used graphics, sound, text, executables or by the techniques used to modify the covers.

- Substitution system.
- Transform domain techniques.
- Spread spectrum techniques.
- Statistical method.
- Distortion techniques.
- Cover generation methods.

AES algorithm is widely used for cryptography. This standard specifies the Rijndael algorithm [17], a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length accepted is 128. To secure the data using cryptography crypto module is used. For crypto module following three steps are used :

- Insert text for encryption.
- Apply AES algorithm using 128 bit key (Key 1).
- Generate Cipher Text in hexadecimal form.

For retrieving the original text from crypto module following steps are used :-

- Get the above retrieved cipher text.
- Reverse AES algorithm by using Key 1.
- Get the original message.

Steganography is the science of hiding information by embedding the hidden i.e. secret message within a cover media in such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media. Steganography hides the fact that the communication does not exist. Steganography differs from cryptography in following way:

- Cryptography techniques have been widely used to encrypt the plaintext data, transfer the ciphertext i.e. unreadable format over the internet and decrypt the ciphertext to extract the plaintext at the receiver side.

- However, with the ciphertext not really making much sense when interpreted as it is, a hacker or an intruder can easily perceive that the information being sent on the channel has been encrypted and is not the plaintext.
- This can naturally raise the curiosity level of a malicious hacker or intruder to conduct cryptanalysis attacks on the ciphertext.

Different types of steganography are as follows :

i. Secret Key Steganography

ii. Public Key Steganography

IV. CONCLUSION

Data security and in particular protection of data from unauthorized accesses remain important goals of any data management system and transmission of data on web to be carried out securely different algorithms are used which are mentioned in this paper. Because transferring of data which is present on web database securely is very important for that all the above mentioned ways are followed.

References

1. Boyens, C., G¨unther, O.: Trust Is not Enough: Privacy and Security in ASP and Web Service Environments. In: Sixth East-European Conference on Advances in Databases and Information Systems. Volume 2435 of Lecture Notes In Computer Science. (2002)
2. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .
3. E.B. Fernandez, R.C. Summers, and C. Wood, Database Security and Integrity. Addison-Wesley, Feb. 1981.
4. P.G. Griffiths and B. Wade, "An Authorization Mechanism for a Relational Database," ACM Trans. Database Systems, vol. 1, no. 3, pp. 242-255, 1976.
5. R. Fagin, "On an Authorization Mechanism," ACM Trans. Database Systems, vol. 3, no. 3, pp. 310-319, 1978.
6. E. Bertino, S. Jajodia, and P. Samarati, "An Extended Authorization Model," IEEE Trans. Knowledge and Data Eng., vol. 9, no. 1, pp. 85-101, 1997.
7. R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-Based Access Control Models," Computer, vol. 29, no. 2, pp. 38-47, 1996.
8. R. Thomas and R. Sandhu, "Task-Based Authorization Controls (TBAC) Models for Active and Enterprise-Oriented Authorization Management," Database Security XI: Status and Prospects, T.Y. Lin and S. Qian, eds., pp. 262-275, 1998.
9. E. Bertino, C. Bettini, E. Ferrari, and P. Samarati, "An Access Control Model Supporting Periodicity constraints and Temporal Reasoning," ACM Trans. Database Systems, vol. 23, no. 3, pp. 231-285, 1998.
10. R. Sandhu and F. Chen, "The Multilevel Relational Data Model," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 93- 132, 1998.
11. S. Bhavana and K. L. Sudha. Text Steganography Using LSB Insertion Method Along with Chaos Theory. International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.2, pp. 145-149, April 2012.
12. T. Morkel, J. H. P. Eloff, and M. S. Olivier. An Overview of Image Steganography. Proceedings of the 5th Annual Information Security South Africa Conference (ISSA2005) (Eds.: H. S. Venter, J. H. P. Eloff, L. Labuschagne, and M. M. Eloff), Sandton, South Africa, 2005. Retrieved from http://martinolivier.com/open/stegoverview.pdf.
13. Hacigümüs H., Iyer B., Li C., Mehrotra S., Providing Database as a Service, International Conference on Data Engineering (ICDE), 2002, pp. 29-39.
14. D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210
15. Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
16. Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002
17. C.E., Shannon, (1949), Communication theory of secrecy systems, Bell System Technical Journal, 28, 656-715.

AUTHOR(S) PROFILE

Sweety Lodha received B.Tech. degree in Information Technology in 2013 from Government College of Engineering Amravati(An Autonomous Institute of Government of Maharashtra) and now pursuing M.E. from Sipna College of Engineering and Technology, Amravati.