A Survey on Securing Databases From Unauthorized Users

Prof. S. S. Asole, Ms. S. M. Mundada

Abstract: - Database and database technologies form a core component of many computing systems and applications which allow data to be stored, retained and shared electronically. As the use of database systems and the amount of data contained in these systems grows continuously and exponentially, database security has become an issue of utmost importance due to an increase in the number of incidents reporting the unauthorized exposure to sensitive data. Hence, the databases should be protected in such a way as to restrict the unauthorized persons from accessing the sensitive contents of database as well as the overall database as a whole. Thus, this paper involves a survey discussing various techniques providing content as well as access security to databases.

Index Terms: - Cryptography, Databases, EVCS, Notifications, Security, Stegnography, Visual Cryptography.

1 INTRODUCTION

WHILE database security encompasses a wide range of security topics as physical security, network security, encryption and authentication, this paper focuses on the concepts and mechanisms particular to the issue of securing the data. This paper discusses techniques to secure the databases concerning a wide range of encryption techniques and discusses a mechanism which provides security to databases from unauthorized users by sending notifications to the authorized users. Thus, this paper involves a survey of various techniques discussing a dual database security problem, that is securing the inner contents of the database and a technique to restrict the very access to the database made by any unauthorized user by sending notifications to the authorized user.

2 NEED OF PROVIDING SECURITY TO DATABASES

Databases are used in various kinds of applications such as surveillances, record keepings in medical fields, military fields, storage of confidential documents in defense systems, criminal related informations in investigation fields, etc. These databases are most vulnerable to unauthorized accesses by eavesdroppers with an intention of stealing the confidential data. Hence there is the need of restricting the very access to the database by unauthorized users along with providing, the security to the inner contents of the database. This dual approach can encapsulate the secret informations in the databases under two protecting covers, that is, restricting access as well as securing the database contents.Therefore a system which makes use of some notifications can be employed which alerts the authorized users of the databases in case of any unauthorized access activity being performed by an unauthorized user with a view of getting an entry into the database and even if someone succeeds to get an entry into database, the contents are not easy to find off as they are secured by some kind of encryption mechanism.

- *Prof. S. S. Asole is currently working as an associate professor in Babasaheb Naik College of Engineering, India, PH- 09764996886.*
  E-mail: suresh_asole@yahoo.com
- *Ms. S. M. Mundada is currently pursuing masters degree in computer science and engineering from Babasaheb Naik College of Engineering in Amravati University, India, PH-09881513139.*
  E-mail: snehal2006193@gmail.com

3 METHODS OF SECURING DATABASES

3.1 Content Security

There are many techniques implemented so far to secure the databases, which mainly involve securing the actual contents within the database by making use of schemes such as cryptography which mainly involves the use of encryption and decryption phenomena applicable to wide range of data in various formats as the textual data, digital video data, images etc. The actual goal of cryptography is to secure the data by changing it in a form that cannot be understood by an eavesdropper [1].Another technique to hide the contents in a database, called steganography, is the art and science of embedding the hidden contents in unremarkable cover media so that it becomes difficult to figure out the very existence of the secret message[1][2].Steganography differs from Cryptography in a sense as where cryptography focuses on keeping the contents of a message secret, steganography focuses in keeping the very existence of a message secret.[6]Apart from these two, there is a third scheme called dynamic steganography which has a blend of both, cryptography and steganography [3] to make the contents of a database secure. Another scheme called visual cryptography is a kind of secret sharing scheme which allows the encoding of secret image into n shares [4]. The visual cryptography scheme is classified into two types depending upon the types and quality of shares produced. One of these is the traditional visual cryptography scheme, also called as threshold visual cryptography scheme, produces meaningless shares hence visual shares cannot be easily identified. This problem is solved by the extended visual cryptography scheme which adds a meaningful cover image in each share [5]. There is also an another implementation called secret image sharing scheme (SISS) which divides the secret image into shadow images(referred to be shadows).If shadows are combined in a specific way, the secret can be revealed[7].

3.2 Access Security

Along with securing the contents, access security is also of utmost importance. The database is a prime focus for attack by an eavesdropper with a view to steal the secret information stored in the database. Hence, the access to the database needs to be restricted so that the intruder doesn't get entry into the database. For this purpose, a notification mechanism is discussed which tracks the unauthorized accesses over the databases. When a person tries to access the database by

entering the username and password, the system sends a notification on the cell phone of an authorized person to make him aware of the unauthorized access taking place to the database.This can restrict the unauthorized person from viewing the contents of the database.

4 TECHNIQUES FOR CONTENT AND ACCESS SECURITY

The following are details of techniques used to provide content security and access security.

4.1 Cryptography

Cryptography is the technique used to avoid unauthorized access of data. Cryptography makes use of encryption and decryption algorithms .It secures the data in such a way that even if any third party tries to interpret the data, he cannot decipher it..The data is transmitted in an encrypted or encoded state, and later decrypted or decoded by the intended party. Cryptography makes use of 'keys' to encrypt or decrypt the data.The security of modern cryptosystems is based on a relatively small amount of information, called a secret key rather than the secrecy of the algorithm.Thus the fundamental goal of cryptography is to provide security to data using encryption mechanism.Cryptography has its applications in ATM systems, computer passwords, etc[9].

4.2 Steganography

Steganography is the art and science embedding the hidden content in unremarkable cover media so that the existence of the secret gets hidden. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography [1]. Essentially, this information-hiding process starts with the identification of a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).[1][8] The embedding process thus replaces these redundant bits with data from the hidden message.

4.3 Dynamic Steganography

Cryptography is a well known method in which the secret message is transformed to another form such that it does not make any sense to the intruder. Where as steganography is a method in which the secret message is hidden inside another file like an image such that the image looks innocent as if it is not carrying any message. If these two methods can be combined together to form a hybrid approach, called dynamic steganography, then two levels of security can be achieved[3].

4.4 Visual Cryptography

Visual cryptography is a kind of secret sharing scheme which allows the encoding of secret image into n shares[4].The secret image can be obtained by stacking the n shares which helps recover the original image.This scheme is classified into two types depending upon the types and quality of shares produced.One of these is the traditional visual cryptography scheme, also called as threshold visual cryptography scheme, produces meaningless shares hence visual shares cannot be easily identified.This problem is solved by the extended visual cryptography scheme which adds a meaningful cover image in each share[5].Thus visual cryptography has numerous applications including visual authentication, identification, steganography and image encryption[10].There is also an another implementation called secret image sharing scheme (SISS) which divides the secret image into shadow images(referred to be shadows).If shadows are combined in a specific way, the secret can be revealed[7].

4.5 Extended Visual Cryptography Scheme

The conventional scheme generates noise-like random pixels to hide secret images because of which one cannot visually identify each share. Hence, there is a need to add a meaningful cover image to each share.[5] The EVCS algorithm used is a novel encryption algorithm for general access structures to cope with the pixel expansion problem. The algorithm is applicable to binary secret images [5]. When the VC-based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of sub-pixels in each constituent share image. Thus, the area of a share is m times that of the original secret image. The contrast of the recovered images will be decreased to 1/m times simultaneously. The pixel expansion problem decreases the contrast of the recovered secret images and also affects the practicability of storage and transmission requirements. To the best known so far, the existing EVCS algorithms for GASs cannot avoid the pixel expansion problem. Therefore, the solution to this problem is proposed in [5].

4.6 Notification System

The notification system aims to provide access security to the databases while all the other above systems discussed serve to provide security to the inner contents of the databases. Every database access can be basically restricted by providing a login in the form of username and password.The username and password, of course, is kept secret so that an unauthorized user cannot get access to database. But sometimes, accidently or intentionally, if an unauthorized person gets aware of the username and password then the database contents can be easily seen.To avoid this, a system can be applied which informs the authorized user about the unauthorized access taking place to the database by sending an appropriate notification, to a device like cell phone, so that such undesired incidents of unauthorized access attempts to the databases can be restricted. This notification system can be directly applied to the databases whose contents are not encrypted or encoded, but it is better to first secure the database contents and then apply the notification system so that the database gets a dual security , that is , access as well as content security. As an example, the application of this notification system to the content secured database of images generated by applying EVCS scheme to the secret images(generated database), as well as, any other application's database which may or may not apply any encryption mechanism to secure its contents, is discussed below. We do not consider any detail implementation mechanisms here as it is a survey paper. Here we consider two kinds of databases.One which is formed by applying an EVCS[5] mechanism to provide first level security, that is, security to the inner contents of the database.In addition to this, a second level of security can be provided by applying the notification system which restricts the access to the database. In EVCS[5], the secret image is broken into I-shares by the encryptor and synthesizer block. The I-shares thus generated are pixel-expansion free.Then a stamping algorithm (stamper) is applied to each share so that the shares can be covered under some meaningful cover image which makes it difficult for the intruder to identify that it is a part of some other secret

image.Also this approach does not introduce any pixel expansion in this phase[5].The resulting shares will be stored in a database whose access is restricted through username and password.When an unauthorized person tries to enter the database by providing the username and password, a notification will be sent to the authorized user over a device like cell phone, so that he becomes aware of some unwanted activity taking place to the database.The right half of the figure considers implementation of notification system to a database formed by any kind of application, which can either consist the data in encrypted form or not. Thus the notification system also can be applied to database of some other application.

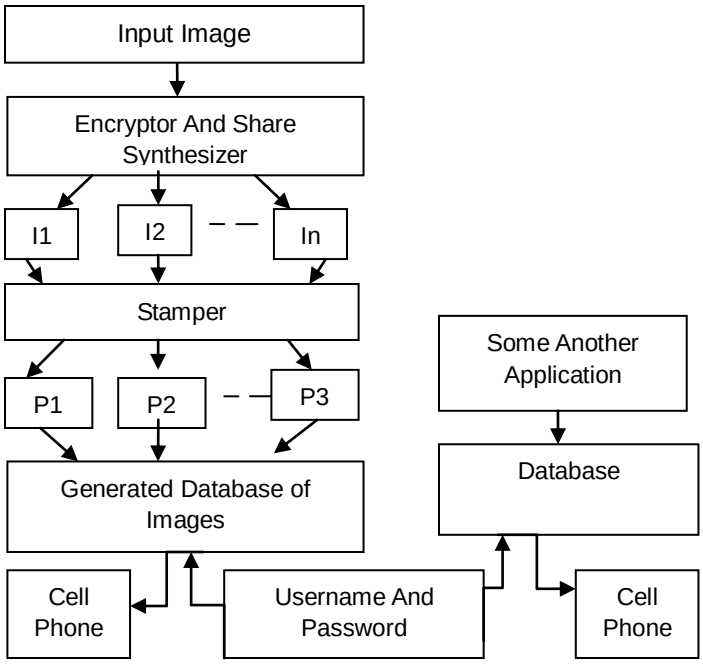

Fig 1: Dataflow Diagram

5 Conclusion

Thus, the paper discusses a survey on securing the databases by providing both, internal security and external security. Internal security can be provided by various techniques as cryptography, steganography, dynamic steganography, visual cryptography, extended visual cryptography, where, basically the overview of extended visual cryptography is studied. A notification system providing the external security to the databases is discussed which makes the databases more secure. Thus, the databases can be made more secure by providing security at two levels, that is, access security and content security.

Acknowledgments

We acknowledge our overwhelming gratitude and immense respect to our Head of the Department, Prof. S. Y. Amdani sir and our Principal, Prof. Dr. K. Ravi sir, who inspired us a lot to achieve the highest goal.

References

[1] Niels Provos and Peter Honeyman, University of Michigan, “Hide and Seek An Introduction to Stegnography”, IEEE Computer Society.

[2] Nagham Hamid, Abid Yahya, R Badlishah Ahmad, Osamah M. Al-Qershi, ”Image Stegnography Techniques: An Overview”, International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012.

[3] Gandharba Swain and Saroj Kumar Lenka, ”A Technique for Secret Communication for New Block Cipher Using Dynamic Stegnography”, International Journal of Security and Its Applications, Vol.6, no.2, April 2012.

[4] Feng Liu and Chuankun Wu, ”Embedded extended visual cryptography scheme” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011.

[5] Kai-Hui Lee and Pei-Ling Chiu, ”An Extended Visual Cryptography Algorithm for General Access Structures”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[6] T Morkel, J H P Eloff, M.S.Olivier”An Overview Of Image stegnogra phy” Information and Computer Security Architecture (ICSA) Research Group. images and videos” IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 48, NO. 8, AUGUST 2000.

[7] Ching-Nung Yang, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn, ”k out of n region incrementing scheme in visual cryptography”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 5, MAY 2012TRANSACTIONS ON SIGNAL PROCESSING, VOL. 48, NO. 8, AUGUST 2000.

[8] Meg Coffin Murray Kennesaw State University, Kennesaw, GA, USA” Database Security: What Students Need to Know ” Journal of Information Technology Education: Volume 9, 2010 Innovations in Practice.

[9] Gaurav Sharma, Ajay Kakkar “ Cryptography Algorithms and approaches used for data security” International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 1 ISSN 2229-5518.

[10] Yu-Chi Chen, Gwoboa Horng, and Du-Shiau Tsai, ”Comment on “Cheating Prevention” in Visual cryptography”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 7, JULY 2012