Database Security Protection Technique Using Position Based Shifting

Miss. Ankita. S. Chikhale
Department of Computer Engineering,
Sipna College of Engineering and Technology
Amravati, India

Prof. S.S. Dhande
Department of Computer Science and Engineering,
Sipna College of Engineering and Technology
Amravati, India.

Abstract-- *This paper primarily aims at the protection of database security when user wants to read that data which is sensitive information for other user to solve the problem associated with this system .There is growing demand for data security of all kinds. Problem concerning to security of database that important information must be secured because in every field security of data is now essential .Cryptography is used for security purpose but for this key pattern is important and in this report gives the idea about the key generation for encryption and decryption purpose. This paper will give an overview of the security of data by matching Semantic Inference Graph (SIG) of encrypted side and decrypted side. By using the position based shifting text; image or audio files are secured by converting in to the encrypted form.*

Keywords:--*SIG, Encryption, Decryption, SIG Matching, cryptography, key generation*

1. INTRODUCTION

Inference is a technique a user can employ to defeat access control mechanisms in a database system. It poses a confidentiality threat to a database system, making it difficult to control access to sensitive information. An inference detection system is needed to determine if users can use legitimately accessed data to infer sensitive information. The design of an inference detection system is a trade among soundness, completeness, accessibility of the database, and efficiency of the inference detection process. ACCESS-CONTROL mechanisms are commonly used to protect users from the divulgence of sensitive information in data sources.

The database inference problem is a well-known problem in database security and information system security in general. In order to prevent an adversary from inferring classified information from combinations of unclassified information, a database inference analyst must be able to detect and prevent possible inferences. Detecting database inference problems at database design time provides great power in reducing problems over the lifetime of a database. In the present time data base security is the main problem. Modern database systems allow multiple users access to data. When users are not to be allowed accesses to every item of data in the database, an access control system is needed. Access control mechanisms are commonly used to protect users from the sensitive information in data sources. An access control system based on two components. The access control policy and the access control mechanism. The access control policy describe the allow are disallowed for each user in data base. The access control mechanism enforces the policy.. In traditional database security research, the database is usually assumed to be trustworthy. Under this assumption, the goal is to achieve security against external attacks (e.g. from hackers) and possibly also against users trying to obtain information beyond their privileges, for instance by some type of statistical inference. However, for many database applications such as health information systems there exist convicting interests of the database owner and the users or organizations interacting with the database, and also between the users. Therefore the database cannot nec essarily be assumed to be fully trusted. 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. 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 strong way to encrypt data or use Semantic Inference Graph for the protection of data .Using strong encryption algorithms Position Based Shifting to encrypt data.

2. LITERATURE REVIEW AND RELATED WORK

2.1. *Human-supplied domain information*

Database inferences have been extensively studied. Many approaches to address the inference problem were presented in [1]. Particularly, Delugach and Hinke used database schema and human-supplied domain information to detect inference problems during database design time [2], [3].

2.2. *Image Encryption using multi level Encryption*

Chang- Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim [17] proposed the multi-level image encryption by using binary phase exclusive OR operation and image dividing technique. The multi-level image can be divided into binary images that have same gray levels. They converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then obtained by combining each binary encrypted image.

2.3. *Schema-level knowledge*

Garvey et al. developed a tool for database designers to detect and remove specific types of inference in a multilevel database system [5]. Both approaches use schema-level knowledge and do not infer knowledge at the data level. These techniques are also used during database design time and not at runtime.

2.4. Tightening Security in Information

Britt focuses the majority of his discussion in the article on the problem of database Security [14]. By examining the current threats and vulnerabilities Britt is able to explore security solutions to selected issues. In providing the security solution, Britt also explains the rationale behind the solution and what security vulnerabilities will be rectified by the solution

2.5. *Digital image encryption algorithm based on chaos and Improved DES*

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [23] researches on the combination of image encryption algorithm like chaotic encryption, DES encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used; it carries on the RGB with this sequence to the image chaotically, and then makes double time encryptions with improvement DES. This algorithm had high security and the encryption speed.

2.6. *Rule-based inference strategies*

Yip and Levitt pointed out the inadequacy of schema-level inference detection, and they identify six types of inference rules from the data level that serve as deterministic inference channels [6]. In order to provide a multilevel secure database management system, an inference controller prototype was developed to handle inferences during query processing. Rule-based inference strategies were applied in this prototype to protect the security [7]. Further, since data update can affect data inference.

2.7. *Inference analysis tool*

Farkas et al .proposed a mechanism that propagates update to the user history files to ensure that no query is rejected based on the outdated information. Hinke et al. developed an inference analysis tool that factors domain knowledge into the inference detection system HDC94, HDW95, DH96. They group inference relevant information into three layers: entity layer, activity layer, and the entity-activity relationship layer [20].

2.8. *Permutation based Image Encryption Technique*

Sesha Pallavi Indrakanti and P.S.Avadhani [24] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provides confidentiality to color image with less computations.

2.9.*Encryption Approach Using a Combination of Permutation Technique Followed by Encryption*

RijnDael was introduced by Mohammad Ali Bani Younes and AmanJantan [25] using the combination of image permutation. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then RijnDael algorithm was applied on the generated image for encryption. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

3. PROTECTION USING CRYPTOGRAPHY

The Information Age has brought with it the ability to share, store, and transmit data with the click of a mouse. The risky part of this equation is that storage and transmission of sensitive data across computer systems can be difficult to protect, increasing the need for vigilance.

Computer systems are complex. They can include operating system software, applications and programs, databases, hardware components, and networks. Each of these elements requires a different method for protecting the data. Adding to the complexity is the dynamism in terms of the way the systems and their parts interact and their requirement for frequent updates to fix bugs or protect against the latest hack attack. All of this collectively underscores the need for each of us to take responsibility to protect the sensitive data we handle.[9] Data in computer systems is vulnerable to similar threats. Threats to secrecy include browsing, leakage, and inference. Browsing refers to searching through main memory or secondary storage for information (e.g., confidential data or proprietary software programs). It is similar to eavesdropping on communication channels, but there are two important differences. On the one hand, information stored in computer systems has a longer lifetime; in this sense, browsing poses a more serious threat than eavesdropping. On the other hand, information transmitted over electronic lines is vulnerable to tapping even when access to the system is denied. Browsing is possible only if the user has access to the system and to unauthorized regions of memory. Access control, can prevent this. Cryptography protects against browsing by making the information unintelligible. It can supplement access controls and is especially useful for protecting data on tapes and discs which, if stolen, can no longer be protected by the system

4. SYSTEM ARCHITECTURE

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security. Data, often referred to as plaintext, is encrypted using an encryption algorithm and an encryption key. This process generates cipher text that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied [17]. Cryptography is the science and study of secret writing. A cipher is a secret method of writing, whereby plaintext (or clear text) is transformed into cipher text (sometimes called a cryptogram). The process of transforming plaintext into cipher text is called encryption; the reverse process of transforming cipher text into plaintext is called decipherment or decryption. Both encryption and decipherment are controlled by a cryptographic key or keys**.** There are number of steps required to protect the information but for protecting this information first we covert the information into the binary format .After converting the information into the binary format we take sampling of this binary format. In this sampling we arrange the binary data into the 8 bits of group. During sampling it gives the total number of samples. After sampling for encryption of this information we generate key pattern .this key pattern are generated by using permutation. Then by using position based shifting algorithm all the information get converted into the cipher text. But for converting this plaintext to cipher text we used keys randomly front key pattern .By using this keys create the SIG (semantic inference graph).this is the encryption side semantic inference graph .when user wants to decrypt that data user have to go through all the steps that previously done by user that is binary conversion then re-sampling. Now for decrypt this we requires that keys which we used for encryption. Semantic inference graph of keys of decryption side when matched with encryption side SIG only then user will decrypt this information. If SIG (semantic inference graph) not 100% match with previous SIG then data will not read by any user.

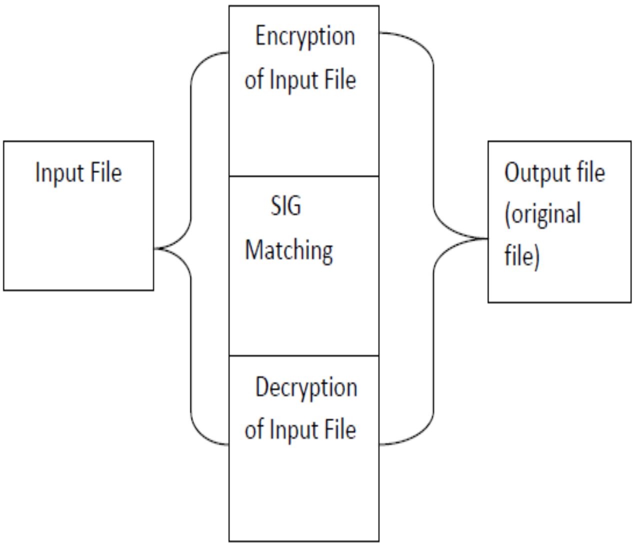


Fig.1 Need of protection using cryptography

5. IMPLEMENTED WORK

Main objectives of this propose work is to protection of information that is text, images and audio.

Proposed system has two main phases :

A. Encryption

B. Decryption

5.1. Binary conversion

Select data, image or audio files to protect that file .When other user read that files at decryption side user need SIG .For this process we need to convert it in binary form.

5.2. Binary Sampling

After converting in to the binary form that binary form are in consecutive way of 0 and 1.In resampling this binary converted to 8 bits of group of samples.

5.3. SIG Creation

To protect that files need to generate key pattern and from that key pattern have to select number of keys for encryption purpose. SIG is semantic inference graph which is drawn from selected keys.

5.4. Encryption

By using this selected keys graph SIG we have to encrypt that files now. By using position based shifting all the information gets encrypted.

5.5 Matching SIG

At decryption side proceed all the steps like above after creation of SIG at decryption side match both the SIG .If both SIG matched 100% then only then decrypt data.

5.6 Decryption

If both encryption and decryption side SIG matched 100% with each other then user can decrypt the data. Otherwise data not converted in original form.

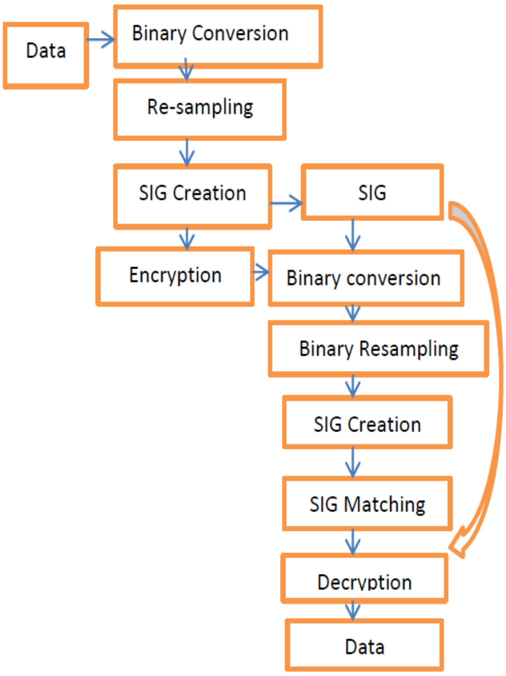


Fig.2 Propose Architecture Design

6. POSITION BASED SHIFTING

For encrypting the data we used position based shifting. In position based shifting generate key pattern that key pattern are generated by permutation. Here information may be text, image, and audio for protecting that information we have to convert into cipher text. Data or any information is represented by number of samples. That every samples or data represented by 8 bit digit. Then vale of every sample is 2^8=256.that is value of every sample is 0 to 255 in the range. After this convert every value of samples in to the binary form but in binary form this is in consecutive manner. By applying the sampling this binary form are arranged in 8 bits of groups. Keys are generated by the position based keys. Position based keys are created by using 0 to 7 digits. By using these digits or by using permutation we generate key pattern. After this we encrypt the data or samples by using those keys from key pattern. If we select 200 keys for encryption and total samples are 100 then 1st sample is encrypted by the 1st key and then 2nd sample is encrypted by the 2nd keys so on in round robin way. Samples or data are encrypted by the exchanging the position of keys data with keys position in round robin manner.

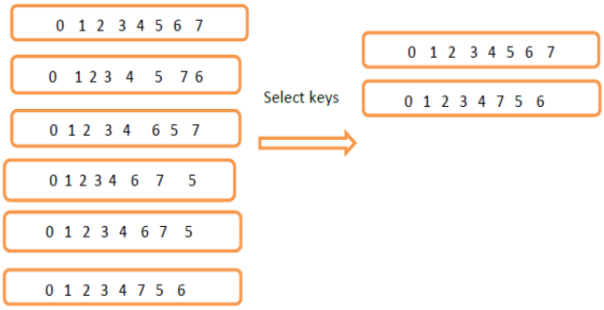


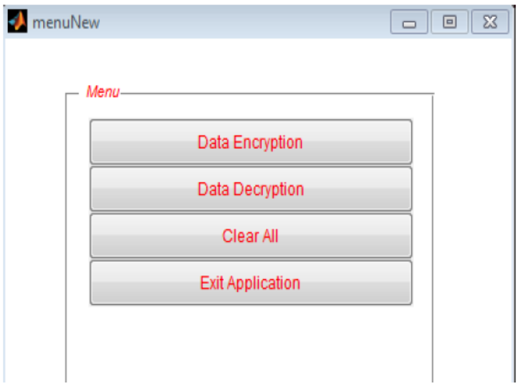
Figure 3 Position Based Shifting

7. RESULT AND DISCUSSION

7.1. ENCRYPTION AND DECRYPTION PROCESS

For encrypting the data we used position based shifting. In position based shifting generate key pattern that key pattern are generated by permutation. Here information may be text, image, and audio for protecting that information we have to convert into cipher text. Data or any information is represented by number of samples. That every samples or data represented by 8 bit digit. Then vale of every sample is 2^8=256.that is value of every sample is 0 to 255 in the range. After this convert every value of samples in to the binary form but in binary form this is in consecutive manner. By applying the sampling this binary form are arranged in 8 bits of groups. Keys are generated by the position based keys. Position based keys are created by using 0 to 7 digits. By using these digits or by using permutation we generate key pattern. After this we encrypt the data or samples by using those keys from key pattern. If we select 200 keys for encryption and total samples are 100 then 1st sample is encrypted by the 1st key and then 2nd sample is encrypted by the 2nd keys so on in round robin way. Samples or data are encrypted by the exchanging the position of keys data with keys position in round robin manner.

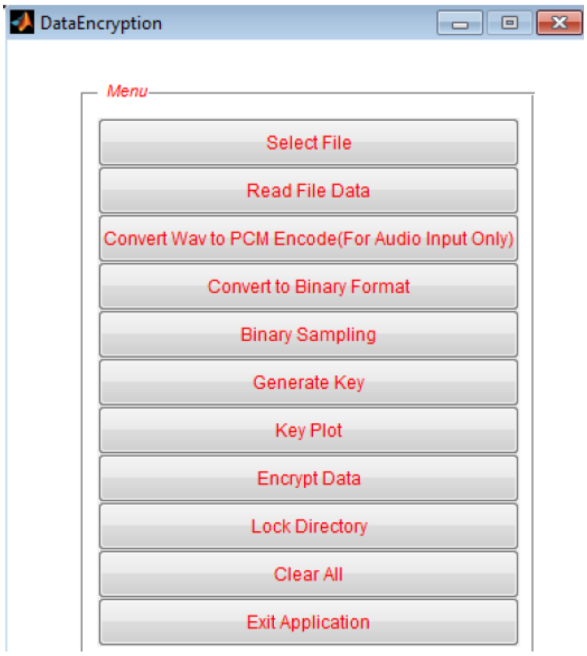
This is main menu where we have to select on data encryption for protecting that file that other user can't read it for this that file must be converted into the cipher text. When user wants to infer that data user must go through the all process of data decryption



Snap shot 1 Overall Process

7.2. DATA ENCRYPTION PROCESS

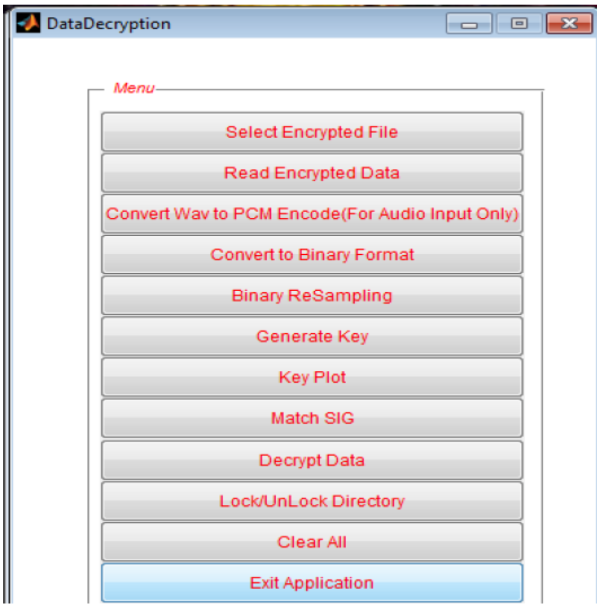
In data encryption process for encrypting the data user have to go through select file, read file convert to binary format, binary sampling, generate key, key plot, encrypt data.



Snap shot 2 Data Encryption Task

7.3. DATA DECRYPTION PROCESS

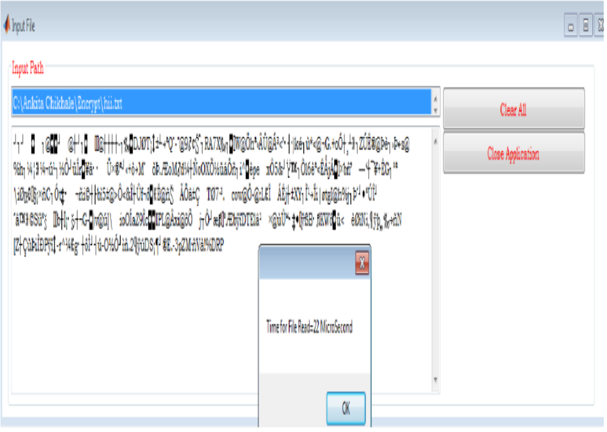
Here the whole decryption process starts where have to select encrypted file for and go through all the process again for decryption process.



Snap shot 3 Data Decryption Task

7.4. ENCRYPTED FILE

This is the encrypted file for database security protection by using position based shifting



C:\Ankita Chikhale\Encrypt\hii.txt

Time for File Read=22 MicroSecond

Snap shot 3 Encrypted

8. CONCLUSION

In this paper we present a technique that prevents users from inferring sensitive information from a series of seemingly innocuous queries. For this we use cryptography for protection of database security .By using position based shifting we protect sensitive information into cipher text. But data will decrypt only when the both semantic inference graph of encryption side and decryption side 100% collaborate or matched with each other otherwise data will not decrypt.

ACKNOWLEDGMENT

It gives me immense pleasure to express my gratitude to Prof. Mrs. S.S.Dhande my guide who provided me constructive criticism and a positive feedback during the preparation of this paper. I also express my sincere gratitude for her support in this paper .Without them and their co-operation of this seminar work would have been inevitable and their presence behind me is totally indispensable.

REFERENCES

[1] C. Farkas and S. Jajodia, “The Inference Problem: A Survey,” SIGKDD Explorations, vol. 4, no. 2, pp. 6-11, 2002.

[2] H.S. Delugach and T.H. Hinke, “Wizard: A Database Inference Analysis and Detection System,” IEEE Trans. Knowledge and Data Eng., vol. 8, no. 1, pp.56- 66, Feb. 2001.

[3] T.H. Hinke and H.S. Delugach, “Aerie: An Inference Modeling and Approach for Databases,” Proc. Sixth Ann. IFIP WG 11.3 Working Conf.

Dataand Applications Security, 2002.

[4] T.H. Hinke, H.S. Delugach, and R. Wolf, “Wolf: A Framework for InferenceDirected Data Mining,” Proc. 10th Ann. IFIP WG 11.3 Working Conf. Data AndApplications Security, 1996.

[5] T.D. Garvey, T.F. Lunt, X. Quain, and M. Stickel, “Toward a Tool to Detect and Eliminate Inference Problems in the Design of Multilevel Databases,”SixthAnn. IFIP WG 11.3 Working Conf. Data and Applications Security, 2005.

[6] R.W. Yip and K.N. Levitt, “Data Level Inference Detection in Database systems,” Proc. 11th Computer Security Foundations Workshop (CSFW ’98),

[7] B.M. Thuraisingham, W. Ford, M. Collins, and J. O’Keeffe, “Design and Implementation of a Database Inference Controller,” IEEE Trans. Knowledge and Data Eng., vol. 11, no. 3, p. 271, June 2009.

[8] C. Farkas, T. Toland, and C. Eastman, “The Inference Problem and Updates in Relational Databases,” Proc. 15th IFIP WG11.3 Working Conf. Database and Application Security, pp. 181-194, 2001.

[9] T.S. Toland, C. Farkas, and C. Eastman, “Dynamic Disclosure Monitor ðD2MonÞ: An Improved Query Processing Solution,” Proc. Second VLDB Workshop Secure Data Management (SDM ’05), 2005.

[10] Raymond W. Yip and Karl N. Levitt: Data Level Inference Detection in Database Systems.

[11] Y. Chen and W.W. Chu, "Database Security Protection via Inference Detection," Proc. Third IEEE Int'l Conf. Intelligence and Security Informatics (ISI '06), 2006

[12] M. Chavira and A. Darwiche, "Compiling Bayesian Networks with Local Structure," Proc. 19th Int'l Joint Conf. Artificial Intelligence (IJCAI '05), pp1306-1312, 2005.

[13] F. Cornelli, E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P.Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th Int'l World Wide Web Conf. (WWW '02), May 2002.

[14] A. Darwiche, "Recursive Conditioning," Artificial Intelligence, vol. 126, 1 2, pp. 5-41, 2001.

[15] A. Darwiche, Class Notes for CS262A: Reasoning with Partial Beliefs. Univ.of California, Los Angeles, 2003.

[16] H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

[17] O. Goldreich, S. Micali, and A. Wigderson. How toplay any mental game | Completeness theorem for protocols with honest majority. In *Proc. 19th ACM Symposium on the Theory of Computing (STOC)*, pp. 218{229, 1987.

[18] M. Hirt and U. Maurer. Player simulation and general adversary structures in perfect multi-party computation. Journal of Cryptology, vol. 13, no. 1, pp. 31{60, 2000.

[19] U. Maurer. Cryptography 2000 *§* 10. R. Wilhelm (Ed.), Lecture Notes in Computer Science, Springer-Verlag, vol. 2000, pp. 63{85, 2000.

[20] U. Maurer. Secure multi-party computation made simple. *Security inCommunication Networks(SCN'02)*, G. Persiano (Ed.), Lecture Notes in Computer Science, Springer-Verlag, vol. 2576, pp. 14 28, 2010.