# Review on Various Techniques of Database Security

[1]Supreet kaur, [2]Dr Sandeep Sharma
*Student- Department of CSE, GNDU,Amritsar, India [1]*
*HOD- Department of CSE, GNDU,Amritsar, India [2]*

***Abstract-***Being safe in today's world is top priority as well as a challenge that humans are in front of all over the world in lives every aspect. Alike security in electronic planet has an immense importance. In this, I survey the protection of database which holds as the crucial/major problem in world of digitalism. Security, integrity and confidentiality of records are demanded on internet for any type of work we do there. Each time the term security gets related to data, the main focus is secure transport of information from one to other end over unreliable network communication. Likewise the database which acts as backbone of any organization needs security as well.

***Keywords*****:** Database Security, Encryption, Access Control, Security techniques, cryptography, hashing, steganography.

## I. INTRODUCTION

Records of any company are a worthless resource. Automation of the record system as well as of operative nature facilities became a must to have need of educational, government aided or social sector as well. According to recent findings it was stated that more than 2 terabyte of e-garbage is produced daily on hourly basis in our unlimited expanding digital world. We human beings use the internet facility for almost our every work; hence the necessity of being safe quadruplet increases on cyber zone. As a matter of fact, internet world is not limited to thought /file sharing only, we do monetary transactions, highly confidential data is being used and send by our intelligent agencies and the list is never ending. In such a scenario there's call for the security as well as certain norms based on which a person could be proved culprit or innocent on his work done over cyber world. When the backend is concerned the key notes as Data protection as well as confidentiality become the top priorities.

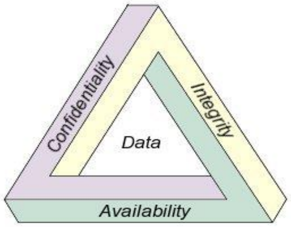


Fig. 1: Properties of Database Security

By the word Confidential simply one means to restrict unwanted access by defining some limits side by side fetching of the data that is secure. Whereas Integrity means that no tainted data we get in any manner and Availability word reflects that right record is at right place at right time( when asked for).By this deliberate effort data is secured not in favor of accidental /intentional loss demolition or mishandling. All threats aim to weakness of reliability of the data along with its access and remoteness of transactions add to difficulty of apprehending the culprit.

The security threats that may prove damaging and catastrophic when disclosed or either accessed publicly are prime concerned area of security of database. Common occurred issues in this security are as:-

- Privilege violence: Due to poor design one may get allotted rights way more than that account actually can have, then these rights can be deliberately or not deliberately exploited.
- Lawful Privilege Abuse: As generally stated "insiders job" here what happens is the lawful access to backend may lead to mistreatment of the data for dangerous motives.
- Privilege endorsement: the clever intruders taking benefits of the loopholes or weak points of the system enters and then raises his level and hence gets his hand on the confidential data of the backend.
- Operating System weakness: the attacker takes benefits of the vulnerabilities/weakness in the operating system such as windows to get illegal right of entry to the backend for malicious reason.

Many database security techniques have been proposed to alleviate these database security attacks. The majority of these methods strengthen the access control mechanisms so as to curb illegal admittance to the backend. In this I mainly focus on issues in security and measures taken to solve those issues of database.

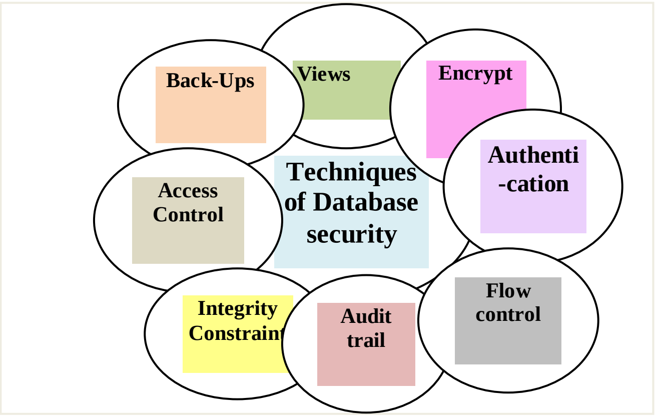
Protecting susceptible data from unlawful access, thievery and forging becomes an immense dispute for different sectors, like government/ no-government as well as privates sectors. The Encryption (the data encoding method) of data on client as well as server side; where information is communal between poles apart parties is not adequate. Fundamentally the hitch is to make certain that semi trusted backend is safe or not. Some familiar protection schemes of database security:-

- Cryptography: the practice as well as study of the techniques wherein the plaintext by encoding (encryption) is transformed to an obfuscated and non-readable content.

- Hashing: the conversion of an uneven length records into a predetermined length string with use of hash functions which makes the retrieval of the data quicker.
- Steganography: process of concealing susceptible information in whichever type of cover medium.
- Access Control: these mechanisms curb the right of entry to the backend along its information to outsiders with the exception of the certified users.

## II. VARIOUS DATABASE SECURITY TECHNIQUES

In this section we list common security database.



Backups provide mirrored copy of the backend preventing from total loss scenario.

- Views works as customized windows with special abilities that put restrict on what can be seen along with what can be done with it.
- Encrypt simply means changing one form to another using some special algorithms and keys.
- Authentication allows giving the lawful users the rights to access the backend.
- Audit trail serves as log where every action done in or on backend is being registered.
- Integrity constraints put a check on data that nothing duplicate, empty, non valid entry gets entered in the backend.

### 2.1 Securing Database via Cryptography

Sesay et al. planned a database encryption system. What happens here was that there were 2 levels of user: Level 1 and Level 2.the first one level user include right of entry to their own personal encrypted information along with the unclassified open information, whereas second level users have right of entry to their own personal data along with classified information which is stored in an encoded format.

While Liu et al. gave a fresh backend encryption means. This mechanism does column-wise encoding thereby allowing the users to categorize the data into susceptible data and open data. This helps in select to encrypt merely that information which is vital leaving the open data intact thereby sinking the trouble of encrypting/ decrypting the whole database records, resulting in enhancement of performance.

A further way is Mixed Cryptography, given by Kadhem et al. This involves crafting a frame to encode the backend over the unreliable system in a diversified outline that encompass of housing many keys by a mixture of parties. The data is made depending upon the possession along with other conditions.

### 2.2 Securing Database via Steganography

Different techniques are there that can be used to conceal significant data in order to prevent them from illegal as well as direct access. The techniques are like still image, audio, video and IP Datagram steganography.

Usually the steganography is used to conceal information. In a scheme the information is implanted in the least significant bits (LBS's) of the values of pixel. The values are numbered into diverse ranges depending on which a definite digit of bits is owed to conceal the sensitive facts. In another scheme the icon is separated into preset amount of blocks. Then Histogram of each one block is considered and the maximum/ minimum points to cover the data. This increases the concealing power. One more advance employs dissimilar approaches which efficiently conceal the sensitive as well as raise the data concealing capacity in still icons. The model involves by means of prime as well as natural numbers to boost the quantity of bit planes to envelop the statistics in the imagery.

### 2.3 Securing Database via Access Control

The planned scheme illustrate as, the right of entry to the backend for a specific stream of video is arranged only after cross checking the credentials of that person. Credentials are not just the user-id but could be the uniqueness traits that identify that particular user and only upon triumphant verification the person is granted the consent to way in the backend.

Kodali et.al gave a universal consent form for MM (multimedia) digital libraries. This involves combining the 3 widely used ACM (access control mechanisms): mandatory, role-based along with discretionary modeling in a single framework as it allows a fused access to the secluded information. This concerns the call for uninterrupted media data along with benefiting the QoS (Quality of service) restrictions along with maintaining the semantics of operational nature.

A proposed model explained technique based on authorization views, enabling authorization transparent querying in which the user queries are formed and represented in terms of database relations and are acceptable only when the queries can be verified using the information contained in the authorization rules. The work presents the new techniques of validity and conditional validity which is an extension of the earlier work done in the same area.

### 2.4 Access Control

Access control ensures all communications with the databases And other system objects are according to the policies and controls defined. This makes sure that no interference occurs By any attacker neither internally nor externally and thus, can Protects the databases from potential errors; errors that can also Make impact as big as stopping firm's operations. It also helps in minimizing the risks that may directly impact the security of the database on the main servers. For example, if any table is accidentally deleted or access is modified the results can be roll backed or for certain files, access control can restrict their deletion.

### 2.5 Inference Policy

Inference policy is required to protect the data at certain Level. It occurs when the interpretations from certain data in the form of analysis or facts are required to be protected at a certain higher security level. It also determines how to protectthe information from being disclosed.

### 2.6 User Identification/Authentication

User identification and authentication is the basic necessity to ensure security since the identification method defines a set of people that are allowed to access data and provides a complete mechanism of accessibility. To ensure security, the identity is authenticated and it keeps the sensitive data safe and from being modified by any ordinary user.

### 2.7 Accountability and auditing

Accountability and audit checks are required to ensure physical integrity of the data which requires defined access to the databases and that is managed through auditing and recordkeeping. It also helps in analysis of information held on servers for authentication, accounting and access of a user.

## III. COMPARATIVE ANALYSIS

If cryptography is implemented to keep the data in the database secure by encrypting the data. Categorizing the users in two levels: Level 1 and Level 2 is done. Based on the Level of the user the accessibility of data is provided. Level 1 user are allowed to access their own private encrypted data and the public data, whereas Level 2 user is permitted to access both, the encrypted private data and the encrypted classified data. The advantage of this scheme is that the grouping of users and grouping of data into two levels avoids the burden of unnecessary encryption of the whole data. Only the classified data and the private data are encrypted and the public data is left unchanged. A rather different approach is to perform column-wise encryption of the data that is defined as the sensitive data by the users. The column-wise encryption approach prevents the whole database to be encrypted but only the critical information, thus averting the performance degradation problem of the database during the retrieval of the data. A varied style is used by the mixed mode of cryptography; it is employed to secure the database over the untrusted and unreliable network in a mixed form. Many keys are held by different parties who have the access to the database so that even when the database is attacked at multiple points by an insider or an outsider the database is not comprised.

The steganography as a method can be implemented to secure the data in the database, in it still images are used to hide the data. In the explained scheme the pixels in the image grouped based on their intensity to hide the data. The advantage possessed by this method is that based on the intensity of the pixels a varied number of bits can be utilized to hide the data instead of fixed number of bits. Instead of grouping the pixels of the complete image based on the intensity, divide the image in equal sized blocks and the histogram of these blocks is calculated. The maximum and minimum points of the histogram are recorded and the critical data is embedded in between these points. The benefit in this approach is that the embedding capacity of the image is enhanced. To achieve the same result of increase the hiding capacity of the image, there is a technique in which prime numbers are used to utilize not just the lower bit planes of the image but even the higher bit planes of the image, thereby extending the hiding capacity.

Authorization techniques for video database are proposed. This includes authorizing the users grouped on their credentials to have access to the video database. The credentials may contain the characteristics defined for the users and not just their user identifications. A stricter approach is to follow the method that involves integrating the mandatory, discretionary and role-based models into a unified framework that grants access to the data in the database. Another technique based on access control mechanism is to use authorization views that enable transparent querying which are validated only when the information is present in the authorization views otherwise they are not. The profit of this approach is that only the records as well as rules present in the authorization views are accepted and only then the access is granted otherwise the access is denied to the database.

## IV. CONCLUSION

Data to any organization is a most valuable property. Database form the backbone of many applications today. They are the primary form of storage for many organizations. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database is vulnerable to number of attacks. In this study security issues faced by databases are identified and some security techniques 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 and less time and space consuming thereby protecting the confidentiality and integrity intact.

## V. REFERENCES

[1] http://en.wikipedia.org/wiki/Database_security

[2] Kayarkar, Harshavardhan. "Classification of various security techniques in databases and their comparative analysis." arXiv preprint arXiv:1206.4124(2012).

[3] Mehrotra, Sharad, and Bijit Hore. "A Middleware Approach for Managing Privacy of Outsourced Personal Data." Department of Computer Science, University of California–Irvine (2009).

[4] Kumar, Vipin, Jaideep Srivastava, and Aleksandar Lazarevic, eds. Managing cyber threats: issues, approaches, and challenges. Vol. 5. Springer Science & Business Media, 2006.

[5] Elisa Bertino, Ravi sandhu, ―Database Security- Concepts, Approaches and Challenges, IEEE Transactions on Dependable and Secure Computing, Vol 2, No 1, January-March 2005 .

[6] Bertino, Elisa, and Ravi Sandhu. "Database security-concepts, approaches, and challenges." IEEE Transactions on Dependable and secure computing2.1 (2005): 2-19.

[7] Shmueli, Erez, Vaisenberg, Ronen, Elovici, Yuval and Glezer, Chanan(2009)Database Encryption- An Overview of Contemporary Challenges and Design Considerations SIGMOD Record vol38, No 3.

[8] Bertino, Elisa, Sushil Jajodia, and Pierangela Samarati. "Database security: research and practice." Information systems 20.7 (1995): 537-556.