International Journal of Advanced Research in Engineering Technology & Science

ISSN: 2349-2819

Email: editor@ijarets.org Volume-9, Issue-7 July – 2022 www.ijarets.org

SECURITY ISSUES IN DATABASE MANAGEMENT SYSTEM

DR. RISHABH GUPTA

OFFICAITING PRINCIPAL

SATGURU INSTITUTE OF EDUCATION AND TECHNOLOGY

ABSTRACT

The suggested approach and the security system of database management systems (DBMS) are the subjects of this study. The customers of a database management system have to have faith that the service providers will have a safe mechanism in place to preserve their information and thwart any attempts by third parties to steal it. Information is a vital component of a database management system. There are just a few different kinds of techniques that may be used to increase the database's level of security. One of the most important and significant difficulties in the field of information and communication technology is database security. This may be broken down into subcategories such as the confidentiality, integrity, and availability of the data and information that is kept in a database. Inaccurate or lost data that is recorded in a database might, under some circumstances, be equated to the loss of a human life.

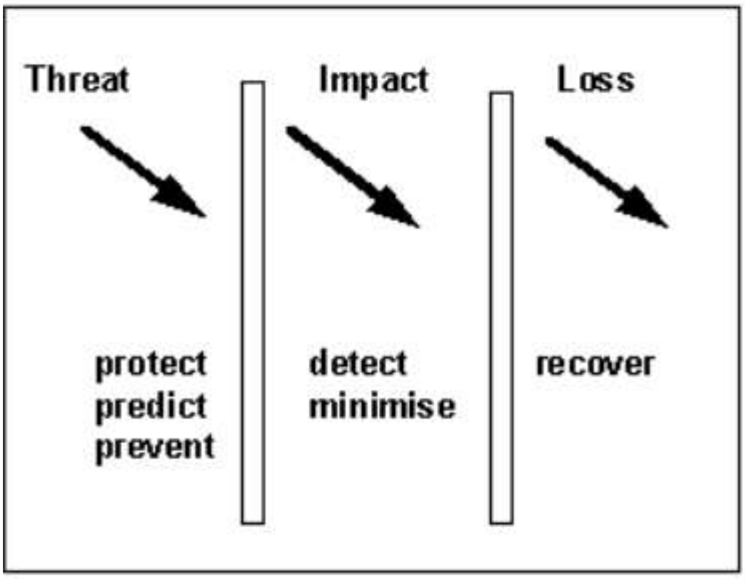
keywords*: Security Issues, Database*

INTRODUCTION

A database is a collection of data that has been organised in such a way that a computer programme may quickly choose desired bits of information from the collection. Users may consider a database to be an electronic documentation structure in their minds. It's a collection of data that customers or authorised users may have access to through a variety of different means. The information is derived from the processed data and saved in the database management system (DBMS). The information is extremely private and sensitive, as it belongs to the clients. When clients supply their information, they do so with the utmost confidence that it will be preserved in a secure manner thanks to the database's security services. It takes more than just protecting the data in a database to devise an all-encompassing plan to keep it safe [4]. The utilisation of security instruments makes it easier for security administrations to notice and prevent a security breach. The protection of the data that is kept in a database is of the utmost importance in order to prevent unwanted access. In addition, the deployment of security services is intended to identify illegal access, detect any assault on information, and contribute to the process of prevention. To protect the data from being hacked or used inappropriately, the necessary procedure ought to be applied. The database administrator is responsible for providing clients with a well-designed system, and only those individuals who have been granted access to the database management system are permitted to log in and add, remove, modify, or update customer information. There are a few different types of methods that can be applied in order to increase the level of security that the information has. Some of these methods include limiting the access control, which requires the user to verify the details with authentication; decreasing the amount of time that is spent accessing the information; and having the data administrator be able to identify the user in order to prevent the user from stealing information while they are accessing the information. In addition to that, including a watermark into the database is a method that may be used to keep the information private while still preserving its integrity. The primary goals are to identify harmful assaults and provide protection for the information owned by the ownership. The use of information that is watermarked can make it more resistant to assaults that include data manipulation and help prevent the change of data that does not need authentication.

The scope of database security

Every system has assets, and the purpose of security is to safeguard those assets. Therefore, the first step is to become familiar with your assets and the worth of each one. Focus your attention in this chapter on database objects like as tables, views, and rows, as well as the access to those items and the larger system that administers them. Take into account that not all data must be protected with extreme caution because not all of it is very sensitive. Each and every asset is in jeopardy. The second item that you need to be aware of is the THREATS that put your assets in jeopardy. Among these are situations like power outages and dishonesty on the part of employees. Take into account the fact that dangers are in part hypothetical, ever evolving, and always only partially understood. All of the security-related activities are geared on shielding the system from any potential dangers. If a danger has the potential to materialise, you have no choice but to prepare for that possibility. The IMPACT of it occurring depends on its being actual. The impact is something you can think about and plan for. On the other hand, if the worst comes to pass, there will be a loss. This security action is aimed towards reducing the amount of data lost, regaining control of the database so as to reduce the amount of data lost, and providing further protection against the same or similar attacks.



An outlined development mechanism is:

1. Document assets (what they are, what their value is).
2. Identify treats (what they are, how likely they are, what the impact is if they occur).
3. Associate threats with each asset.
4. Design mechanisms to protect each asset appropriate to its value and the cost of its protection, to detect a security breach against each asset, to minimise the losses incurred and to recover normal operation.

Threats to the database

Both fronts will contribute to the development of your security expertise. One stems from an appreciation and understanding of evolving hazards, while the other stems from the development of technical solutions to counteract such threats. Among the dangers are:

- **Unauthorised modification:** The alteration of data values for the purpose of sabotage, criminal activity, or simple ignorance, which may be made possible by insufficient security procedures, such as the sharing of passwords or the guessing of passwords, as an example.
- **Unauthorised disclosure:** when information that should not have been made public was inadvertently made public. A widespread problem of critical significance, which may have been caused by mistake or on purpose.
- **Loss of availability:** Occasionally referred to as denial of service. In the event that the database is unavailable, it results in a loss (otherwise, life would be much better without the system!). Therefore, it is important to eliminate any potential hazard that might result in time spent offline, even if it is just to check whether something has taken place.

The rest of this section is an overview of the categories of specific regulatory threats to database systems.

- **Commercial sensitivity:** The majority of a company's financial losses due to fraud are caused by workers. Access controls offer two benefits: protection against illegal activities and proof of efforts (successful or not) to carry out activities that are harmful to the organisation. These activities might include fraud, the extraction of sensitive data, or a loss of availability.
- **Personal privacy and data protection:** Generally speaking, personal information is subject to governmental constraints on a global scale. Personal data is data about an identifiable individual. Usually, the person being identified needs to be alive, but there is no set procedure for determining their identity. If there is just one person living at the address associated with the postal code, then it is possible that the individual can be identified using the postal code for the residence. The management and administration of such data requires extreme caution.
- For more information see Data Protection later in the chapter. The issues are too extensive to be discussed here but the implications should be noted. Personal data needs to be identified as such. Controls must exist on the use of that data (which may restrict ad-hoc queries). Audit trails of all access and disclosure of the information need to be retained as evidence.
- **Computer misuse:** In most countries, there is additional regulation regarding the inappropriate use of computers. Misuse encompasses both the violation of access rules and the effort to inflict harm by either altering the state of the database or introducing worms and viruses in order to disrupt the normal functioning of the system. These types of offences frequently allow for extradition. Therefore, unauthorised access in Hong Kong to databases in Germany using computers in France to access German databases that relate to American databases might result in extradition to either Germany, France, or the United States.
- **Audit requirements:** These are operational restrictions based on the requirement to know who did what, who tried to do what, where everything happened, and when it occured. They entail the detection of events (such as CONNECT and GRANT transactions), the provision of evidence for the detection, assurance, and either defence or prosecution of an activity, and the provision of evidence. There are concerns with computer-generated evidence that are not addressed in this article.

It is easy to lose sight of the reality that every access to the system has with it inherent hazards when one is considering logical access to the database. If one has access to the utilities of the operating system, it is then feasible to directly access the storage on the disc and either copy or corrupt the database in its whole or any of its individual parts. A complete consideration has to take into account all of these different entry points. The vast majority of analysts will try to restrict communications (direct, network, and telecommunications) as much as possible and try to isolating the system from any needless dangers. Encryption is another possibility, and it's possible that it'll be applied to both the data and the schema. The process of transforming text and data into a form that can only be read by the intended recipient of that data or text, who must know how to convert it back to a clear message in order to decipher it, is referred to as encryption. You will find it much simpler if you think about security and auditing as challenges that are distinct from the primary operations of the database, regardless of how those functions are implemented. Consider the security server and the audit servers to be two distinct functional modules.

Principles of database security

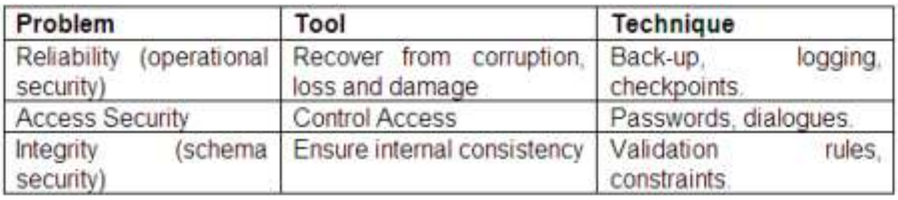
You need a model of security in order to arrange your views on security. These can take a variety of shapes, depending on the roles involved, the degree of information required, and the goal. The primary categories consist of the aspects of concern (threats, impacts, and losses), as well as the activities associated with mitigating those aspects.

Security risks are to be seen in terms of the loss of assets. These assets include:

- Hardware
- Software
- Data
- Data quality
- Credibility
- Availability
- Business benefit

In this context, our primary concern is with threats to the data and the data quality; nonetheless, it is only natural that a danger to one asset would have an effect that ripples through to other assets. Always make sure that you have a firm grasp on precisely which assets require protection before taking any action.

So as a summary:



Problem	Tool	Technique
Reliability (operational security)	Recover from corruption, loss and damage	Back-up, logging, checkpoints
Access Security	Control Access	Passwords, dialogues
Integrity (schema security)	Ensure internal consistency	Validation rules, constraints

You have to come to terms with the fact that there is no such thing as foolproof security. There is always some element of risk, therefore preparations need to be taken to cope with the worst-case scenario. This includes taking measures to reduce the impact of any adverse events and efficiently recover from the destruction or loss of any assets. Consider the following aspects:

1. Appropriate security - you do not want to spend more on security than the asset is worth.

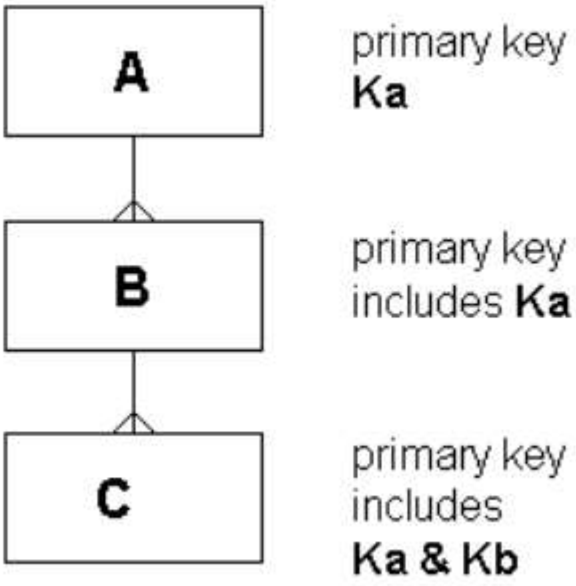
2. You do not want security measures to interfere unnecessarily with the proper functioning of the system.

Database security issues

In this part, some of the challenges that might be encountered while developing the security specification for a database system and putting it into action are discussed.

Access to key fields

Let's say you have a user role that gives you access to table A and table C but not table B. What would you do? The issue is caused by the fact that the columns from B are included in the foreign key in C. There are a few questions that come to mind:



Have you looked at getting access to the foreign key in C? If this is the case, you are aware that at the very least a tuple exists in B and that you have access to some information about B that you are not supposed to have. Are you able to update the columns that include the foreign keys? In that case, it is required to cascade, resulting in an update being made to B for which no rights have been assigned. When the database is implemented by using internal pointers, these concerns do not immediately emerge; as a user, you do not need to have any knowledge of the relationships between the data that you are accessing. They manifest themselves due to the fact that relationships are data values. In many cases, having the foreign key will not in and of itself constitute sensitive information. If such is the case, the problem could be solved by rethinking the definition of a view.

Access to surrogate information

It is not difficult to conceive of cases where the view of the data provided to a user role extends to the external world.

An example should make the problem clear.

The retail industry is plagued by persistent issues of shoplifting and other forms of theft. In order to cope with these issues, private investigators often operate covertly. They are, for all means and purposes, employees of the company and are given the same responsibilities in the daily operations of the firm as other members of the workforce. They receive their pay checks or pay slips at the same time as everyone else, and they are accounted for in the same manner in management information (such as the wage analysis). They engage in the system as someone else while holding a work title that belies their true identity. Everyone, with the exception of the manager of the company's corporate security, is in the dark about the issue. This includes the manager of the shop. When the manager of the store enters the database, the investigator should appear to be a regular employee. Possible questions are as follows:

“What leave is due to …?” The security staff have different queries: “Do we have someone in …?”

You are probably able to foresee a variety of different challenges. The detective ought to be given a pay stub along with the rest of the employees, but he or she should not really be paid (or perhaps the detective ought to be paid something else than the typical salary for the position). You could find it more convenient to manage these scenarios on distinct databases. It's possible that this might work as a remedy, but the more complex the issue is, the more room there is for misunderstanding. The polyinstantiation of tuples is one approach that has been proposed; in this technique, a single individual is represented by more than one tuple. The security categorization of the user will determine which data may be retrieved from the system. Tuples will have the same seeming main key but separate real primary keys, and all applications will need to be connected with the security mechanism in a thoughtful manner.

RELATED WORKS

There are many other strategies for ensuring the safety of database management systems; however, the watermarking for ownership strategy is the one that will be discussed here. During an assault on the database that is maliciously intended to steal data, the owner can secure the data by introducing a watermark picture into the database. In this research, we examine a strategy for watermarking relational databases using binary images as the watermark [1]. This technique uses binary images as the watermark. In addition to this, database encryption is the process of converting information included inside a database management system from its plain text configuration into an unimportant figure message using techniques for the suitable computation. The data have just a minimal level of encryption, making them susceptible to a wide variety of assaults that do not require knowledge of the decryption keys [2]. Decrypting a database involves converting the meaningless figure material back into the original data by employing the keys that were generated by the encryption computations. Encryption and decryption are used for the goal of preserving the data integrity of customers and protecting the confidentiality of the data being transmitted to consumers through the use of database security services. Encrypting data serves the purpose of preserving the secrecy of the information it protects [2]. In addition to this, the data that is being stored in a secure manner is encrypted using the SecCloud protocol [5]. Information may be kept private inside cloud services if the access control is restricted and a record of all information is kept. This helps to ensure that the cloud's security is not compromised. In spite of the fact that cloud services do not require a significant financial investment, there is a significant risk to the data's security, confidentiality, and integrity as compared to physical database management systems (DBMS). Because of the cloud computing system's high degree of complexity and its dynamic resources, which users may access via a diverse set of authentication methods, it might be challenging to spot malicious attacks on the system. This research intends to provide an additional layer of safety so as to lessen the likelihood of unauthorised users gaining access to data [3]. During the designing process, it demonstrates the method of reducing limitations by merging the information depending on the sensitivity degree of each piece of data. The architecture of a database system has to be created with the data integrity and security mechanism as the primary design considerations. Use this document as a template and just write your own material into it to easily conform to the formatting criteria for the conference paper. This is a simple approach to meet the standards.

PROPOSED METHOD

The fast advancement of digital technology in today's world has resulted in a rise in the amount of data that has been duplicated or altered, including text, images, audio, and video. The duplication of data in a digital system can result in the generation of new data that almost exactly resembles the original data. Figure 1 presents the suggested structure that will be used to prevent the alteration of data as well as the duplication of that data within the database security management system (DBMS). By incorporating watermarking into the database, this technique seeks to achieve its primary objective, which is to safeguard the ownership of the data. The characteristics of the database will include a binary representation of an image along with some text added into it. After that, data will be included into the invisible watermark picture so that it may be used for copyright purposes. The information will be encrypted before being concealed within the system. Following then, the data that has been encrypted will be kept and processed. Therefore, it is necessary for the user to encode the data with the alpha-numeric characters of the secret key. On the other hand, the extraction of data won't take place until after the ownership of the relevant data has been verified. In order for the system to be able to decrypt the data and perform access control, the user is required to give accurate information. The addition of a watermark will not render the database's primary information inaccessible in any way. When an individual submits their data to a system, they have the ability to apply watermarking techniques themselves. Before beginning the process of embedding, the encryption technique will first complete the task of constructing the watermark algorithm. We are going to add a watermark on the primary database, and then we will return it with the marked [1] designation. The information in its original form will retain both its secrecy and its integrity when using this approach. In addition, the implementation of a multimedia watermark is simple, making it ideal for huge attribute sets of data, where it can help to increase data privacy.

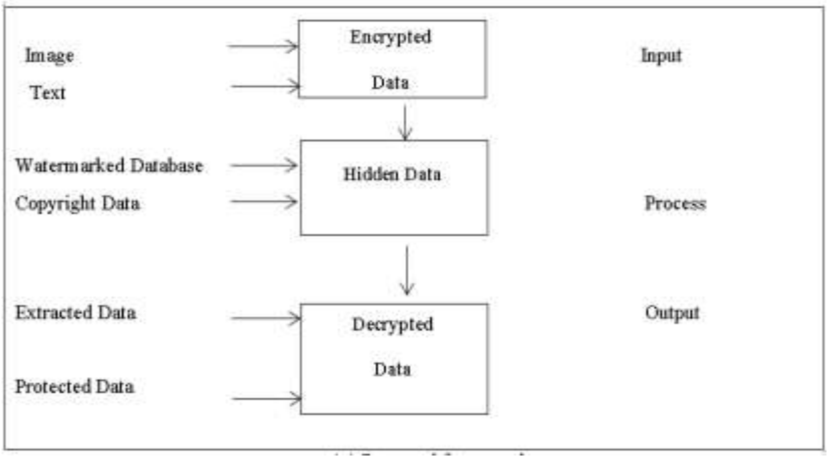
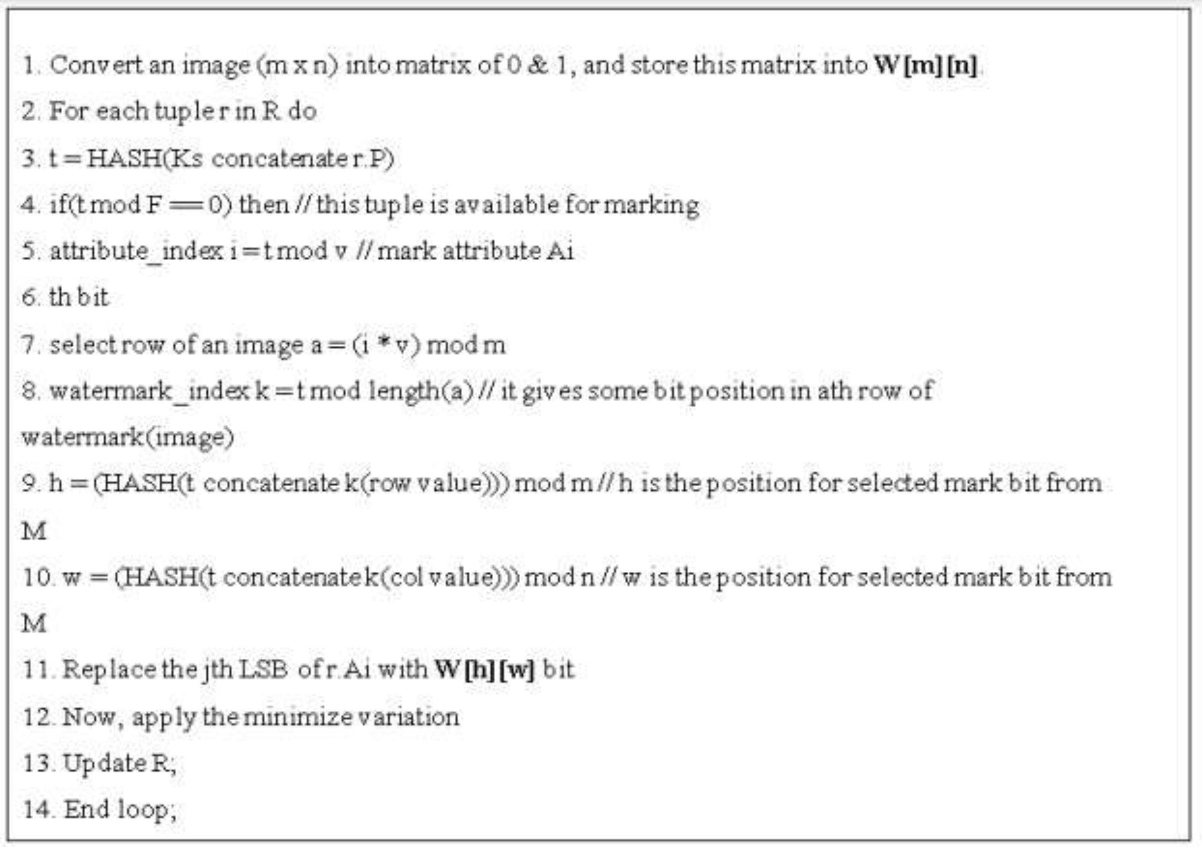


Fig 1. Proposed Data Ownership Protection via DBMS



```
Convert an image (m x n) into matrix of 0 & 1, and store this matrix into W[m][n]
For each tuple r in R do
t = HASH(Ks concatenate r.P)
if(t mod F == 0) then // this tuple is available for marking
attribute_index i = t mod v // mark attribute Ai
th bit
select row of an image a = (i * v) mod m
watermark_index k = t mod length(a) // it gives some bit position in ath row of watermark(image)
h = (HASH(t concatenate k(row value))) mod m // h is the position for selected mark bit from M
w = (HASH(t concatenate k(col value))) mod n // w is the position for selected mark bit from M
Replace the jth LSB of r.Ai with W[h][w] bit
Now, apply the minimize variation
Update R;
End loop;
```

Fig 2. Watermark Algorithm [1]

DISCUSSION

In this investigation, the method that was suggested has the potential to be useful for future efforts that aim to develop a database protection mechanism utilising novel ways. Despite this, watermarking techniques are extensively employed to protect multimedia data from being altered or copied, including audio tracks, movies, and photographs. The vast majority of multimedia data is also kept in the system that manages databases. There are several varieties of watermarking, each providing a unique level of protection. It is contingent on the most important aspect of these facts. Users will be able to reap the benefits of the computer system if it is not too expensive and if it is constructed with the appropriate mechanism. In addition to this, an image-based watermarking approach was suggested since, during the first step of the process, the picture will be inserted and then converted into a scrambled image. Because of the data processing level, ownership is the primary concern when it comes to watermarking. This is because parts of the watermark can be removed or deleted by an unauthorised person. In addition, an integrated watermark may be utilised for a biometric scan of the content owner alone, and it can prohibit the material from being distributed without the owner's knowledge or consent. If the relevant database system has a security policy, the owner may submit a claim for the protection of the content's copyright in this scenario. Additionally, watermarks have the option to identify any tampered or altered data. It is essential to make certain that the data's integrity is verified through the data's integrity once it has been extracted. When the content of a database is utilised for extremely fundamental applications, for example, business exchanges or therapeutic applications, it is essential to guarantee that the data is obtained from the correct source and has not been manipulated. This is particularly important when the database content is used for extremely basic applications. Putting a watermark in the essential information of the database is one way to achieve this goal. There are two primary categories of watermarking methods, which may be broken down into more specific categories as watermark embedding and water verification. The embedding approach is the initial stage, which entails inserting the secret key into the database such that it is freely available and not subject to access restriction. The data cannot be embedded using the watermark approach since this requires precise computing and calculation to be carried out. In the second step of the process, which is dedicated to validating the credibility of the material, the user will be asked to supply the correct secret key in order to get the information from the database. The resilience of the watermarking method is put to the test by a wide variety of harmful assaults.

CONCLUSIONS

To be more specific, the research provide light on the many methods that may be used to raise the overall degree of protection afforded by a database management system (DBMS). Using this strategy, the suggested method seeks to determine whether or not the secrecy of the data can be effectively measured. The user is able to have safeguarded data, free from alterations and duplicates, thanks to the contributions made by the approach. In addition to that, the algorithm approach is utilised in the development process by a large number of data administrators. In addition, the watermarking method has the potential to be implemented in cloud computing services as a high-security solution in the not too distant future. Finding different ways to safeguard one's ownership is a task that is both essential and difficult to complete. The proposed method is amenable to assessment through the utilisation of database experimental testing.

REFERENCES

[1] U.P. Rao, D.R. Patel, and P.M. Vikani, “Relational Database Watermarking for Ownership Protection,” Procedia, 6, pp. 988-995 Technology, 2012.
[2] M. Şerban, “Methods to Increase Search Performance for Encrypted Databases,” Procedia Economics and Finance, 3, pp. 1063-1068 (2012)
[3] D. Trivedi, P. Zavarsky, and S. Butakov, “Enhancing Relational Database Security by Metadata Segregation,” Procedia Computer Science, 94, pp. 453-458, 2016.
[4] T.D. Vale, “Principles of Security and Integrity of Databases,” 15, pp. 401-405, 2014.
[5] N. Vurukonda and B.T. Rao, “A Study on Data Storage Security Issues in Cloud,” Computing. Procedia Computer Science, 92, pp. 128-135, 2016.
[6] M. R. Shinde, “Overview of Database Security,” vol. 5, no. 6, pp. 7920–7921, 2014.
[7] J. Van Loon, “Database Security Concepts and Approaches,” 2017.
[8] R. Elmasri and S. B. Navathe, Fundamentals of Database Systems, Fourth Edition. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2003.
[9] P. R. Patel, “Database Recovery Techniques : A Review,” vol. 4, no. 4, pp. 11482–11486, 2015.