International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228620

Analyzing Database Security and A Study of Ownership Protection using Watermarking Algorithm

Saikat Baul*, Md. Ratan Rana

Department of Computer Science, American International University-Bangladesh, Dhaka, Bangladesh

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 208-216

Article History
Accepted: 10 Nov 2022
Published: 20 Nov 2022

ABSTRACT

This paper is an analysis of database security and a study of ownership protection using the watermarking algorithm. Information is a crucial component of a database, and customers rely on service providers to have a solid system in place to guard against malicious attacks and data breaches. To boost the database security level, a few different types of approaches are used. The watermarking algorithm is one of those approaches. Digital watermarking is an important sub-field of information concealment technology research. It is a technology that incorporates identifying data into digital works. To protect digital product copyright, the basic idea is to embed confidential information in digital products such as images, audio, and video to achieve data fusion. The current digital watermarking technology has made significant progress in the field of multimedia information (such as images, audio, and video). It is resistant to frequent database attacks.

Keywords: Database Security, Ownership Protection, Watermarking Algorithm

I. INTRODUCTION

A database is an assortment of information coordinated so that a computer program can rapidly choose desired bits of information data. A database can be thought of as an electronic documentation framework. It is a collection of data that clients or authorized users can access in a variety of ways. In a database management system, data is processed and stored as information. Client information is highly confidential and proprietary. Clients provide information with confidence in the database's security services, knowing that the information will be safely stored. A comprehensive database security strategy entails more than just data security [1].

The use of security instruments assists security administrations in recognizing and containing a security attack. The security of data stored in a database is critical to prevent unauthorized access. Furthermore, the implementation of security services is to identify unauthorized access, detect any information attack, and be a part of the prevention process.

To protect data from hacking or misuse, an appropriate method should be used. Data administrators must provide a well-designed system for clients and individuals with authorization to login to the database management system and perform CRUD operation. There are a few methods that can be used to increase the security level of information, such as limiting access control so that the user must verify the details with authentication, reducing the time it takes to access the information, and identifying the user to prevent information theft during the access time. Furthermore, watermarking into databases can be used to maintain the confidentiality and integrity of information. The emphasis is on detecting malicious attacks and protecting information ownership. Watermarking information can make it more resistant to data manipulation attacks and prevent data modification without authentication.

The prominence of World Wide Web showed the business capability of offering media assets through the advanced organizations. Since business interests try to utilize the advanced organization to offer computerized media for benefit, they have major areas of strength for an in safeguarding their possession privileges. The computerized information can be handled, gotten to, and it tends to be sent rapidly utilizing networks. There are various specialized, lawful, and authoritative issues which emerge when there is wide scale utilization of advanced reports.

II. BACKGROUND OF THE STUDY

There are several techniques for securing database management systems; the proposed technique is watermarking for ownership. During a malicious attack to steal data, the owner can protect the data by inserting a watermark image into the database. In this paper, we research a strategy for social database watermarking that involves a parallel picture as the watermark [2]. Furthermore, database encryption is a method of converting information within a database management system that is in plain text format into an unimportant figure message using appropriate calculation methods. Weakly encrypted data are helpless against different assaults that don't require admittance to unscrambling decryption keys [3]. Database decryption is the process of converting random number content into original data using keys generated by encryption calculations. The goal of encryption and decryption is to protect the confidentiality of data and to maintain customer data integrity through database security services. The purpose of data encryption is to ensure data confidentiality [3]. Furthermore, the “SecCloud” protocol employs encryption to secure data storage [4]. To maintain the security of information in cloud services, limit access control and keep a track record of information. Although cloud services are not expensive, the security, confidentiality, and integrity of the data are not as secure as with a physical database management system. Because of the complexity level and dynamic resources that can be accessed using a variety of authentication methods, it is difficult to identify malicious attacks on cloud computing. By adding an extra layer of security, this study hopes to reduce the risk of unauthorized data access [5]. It demonstrates a technique for combining information based on its sensitivity level during the design phase to reduce constraints. A database system's architecture must be designed with data integrity and security in mind. Involving this record as a layout and just composing your text into it is a simple method for consenting to the gathering paper designing necessities.

III.DATABASE SECURITY

A database's confidentiality, integrity, and availability are established and maintained using various tools, controls, and security measures. This article will concentrate on confidentiality because it is the most compromised element in data breaches. The following must be addressed and protected by database security:

- The database's information
- The database administration system (DBMS)
- Any related applications
- The physical or virtual database server, as well as the underlying hardware

- The computing and/or network infrastructure that is used to connect to the database.

Database security is a challenging and complicated task that involves all facets of information security practices and technologies. It's also incompatible with database usability. A database can be more vulnerable to security threats when it can be accessed and used easily. When a database is more secure, it is difficult for attacker to access and use it.

A. *Importance of Database Security*

A data breach is defined as a failure to maintain the confidentiality of data in a database. The extent of the damage caused by a data breach depends on several consequences or factors, including:

1) Intellectual property has been compromised: Trade secrets, inventions, and proprietary practices may be essential for maintaining a competitive advantage in your market. If your intellectual property is stolen or exposed, it may be difficult or impossible to maintain or recover your competitive advantage.

2) Brand reputation damage: Customers or partners may be hesitant to purchase your products or services (or do business with your company) if they do not believe they can trust you to protect their or your data.

3) Business continuity: Some companies are unable to continue operations until a breach is resolved.

4) Penalties or fines for non-compliance: Global regulations like the Sarbannes-Oxley Act (SAO) or the Payment Card Industry Data Security Standard (PCI DSS), industry-specific data privacy regulations like HIPAA, or regional data privacy regulations like Europe's General Data Protection Regulation (GDPR) can have crippling financial repercussions with fines exceeding several million dollars per violation.

5) Repair and notification costs: In addition to the cost of communicating a breach to customers, a breached organization must pay for forensic and investigative activities, crisis management, triage, and repair of the affected systems, among other things.

B. *Common Threats and Challenges*

Many software misconfigurations, vulnerabilities, or carelessness or misuse patterns can lead to breaches. Some of the most common types and causes of database security attacks are as follows.

1) Insider Threats: Insider threat refers a security risk that can be posed by any people with privileged access to the database, such as a negative insider who has malicious intentions, a negative insider who makes mistakes that make the database vulnerable to attack, or an infiltrator, who is an outsider who obtains credentials through phishing attacks or by accessing the credential database itself.

One of the most frequently cited reasons for database security breaches has been insider threats, which frequently arise from giving excessively many employees access to privileged transactions.

2) Human Error: Most of the (49%) reported data breaches are caused by silly mistakes, poor passwords, unauthorised password sharing, and other careless or naive user behaviours.

3) Exploitation of Database Software Vulnerabilities: Hackers make a living by identifying and exploiting vulnerabilities in various types of software, including database management software. All significant commercial database software providers and open-source database management platforms regularly release security patches to address these vulnerabilities; however, failure to apply these patches on time can increase your exposure.

4) SQL/NoSQL Injection Attacks: These are database specific threats in which arbitrary SQL or non-SQL attack strings are inserted into database queries served by web applications or HTTP headers. Organizations that do not adhere to secure web application coding practices or conduct regular vulnerability testing are vulnerable to these attacks.

5) Buffer Overflow Exploitation: A buffer overflow arises whenever a system transfers additional data than what a fixed-length memory block can accommodate. Attackers might execute attacks utilizing spare data at adjacent memory addresses.

6) Denial of Service (DoS/DDoS) Attacks: In a denial of service (DoS) attack, the attacker floods the target server—in this case, the database server—with so many requests that the server is unable to fulfill legitimate requests from actual users and, in many cases, crashes. The deluge in a distributed denial of service (DDoS) attack comes from multiple servers, making it more difficult to stop the attack.

7) Malware: Malware is software that is designed to exploit vulnerabilities or otherwise harm a database. Any gateway device may compromise the database network.

8) Attacks on Backups: Backup-related attacks potentially assault enterprises that don't safeguard data backups by applying the same standards as the database. These dangers are exacerbated by the following factors:

- Increasing data volumes: Data capture, storage, and processing are expanding at an exponential rate across nearly all organizations. Data security mechanisms must be flexible to satisfy current and long-term requirements.
- Infrastructure Expansion: Network environments are becoming more complex, especially as businesses shift workloads to multi-cloud or hybrid cloud architectures, making the selection, deployment, and management of security solutions more difficult.
- Increasingly stringent regulatory requirements: As the global regulatory compliance landscape becomes more complex, adhering to all mandates becomes more difficult.
- Cybersecurity skills shortage: Experts predict that by 2022, there may be up to 8 million unfilled cybersecurity positions.

C. *Best Practices*

Any security threat to any component or section of the network infrastructure is likewise a danger to the database. Additionally, any attack that impacts a user's device or workstation may harm the database. This is since databases are nearly always accessible through the network. As a result, database security must go far beyond the database itself.

Consider the following areas when evaluating database security in the environment to determine team's top priorities:

- Physical security: Whether on-premises or in a cloud data center, the database server must be housed in a secure, climate-controlled environment. If the database server is hosted in a cloud-based data center, the cloud provider will be liable for taking care of this for clients.
- Administrative and network access controls: Only the bare minimum of users should have access to the database, and their permissions should be limited to the bare minimum required for them to do their jobs. Similarly, network access should be restricted to the bare minimum of permissions.
- Security of end-user accounts and devices: Always keep a very close eye on whoever is accessing the system, as well as when it is being accessed and how the information is being used. The administrator could well be informed by automatic monitoring systems if data activities seem to be dangerous or unusual. At all times, every user device that communicates to the database network has to be susceptible to security rules and must be entirely safe (meaning that it should only be in the hands of the proper user).
- Encryption: While at rest and in transit, ALL data including database data and credential data should be protected with best-in-class encryption. All encryption keys should be handled in accordance with industry best practices.
- Security of database software: Assure that the database management application is updated to

the most current version and install all fixes as soon as they become available.

- Application/web server security: Any application or web server that interacts with the database can be an attack vector and should be subject to ongoing security testing and best practice management.
- Backup security: The original database as well as any backups, duplicates, or representations of the database need to comply to the same security measures as the original database.
- Auditing: Keep track of all logins to the database server and operating system, as well as all operations performed on sensitive data. Audits of database security standards should be performed on a regular basis.

IV. DATABASE WATERMARKING

A. *Introduction of Database Watermarking*

Database watermarking is the process of embedding imperceptible and difficult to remove tags in a database using signal processing without affecting the database's content or availability, to protect the database's security. Under the premise of safeguarding database security, it cannot harm the database's contents or availability [8] [9].

Watermark signals embedded in databases can be seen as a strong background superimposed on a weak signal if the superimposed watermark signal strength is less than the database availability's allowable distortion threshold. The watermark signal may be placed in the database without meeting concealment and availability criteria.

Database watermark embedding can be thought of in terms of digital communications as a narrow-band signal (watermark) on a wide-band channel (carrier database) that employs spread spectrum communication technology [6]. Although the watermark signal contains a certain amount of energy, it is difficult to detect the energy distributed to any frequency in the channel. Watermark decoding (detection) is a problem of detecting weak signals in a noisy channel. The database watermarking system is divided into four sections: watermark generation, embedding, extraction, and detection. Key control is used to generate the watermark signal, which is typically a binary bit sequence [6].

The watermark signal may include information that is adaptable, which may be used to extract features of the database; it may also include information about the data owner, such as a trademark logo or copyright text; it must generally, be processed prior to signal conversion; and then used to generate watermark signal. The watermark channel with key participation is obtained by extracting the feature of the relational data and applying appropriate transformation processing. The embedding and detection of watermark signals are performed under key control, as illustrated in Figure 1.

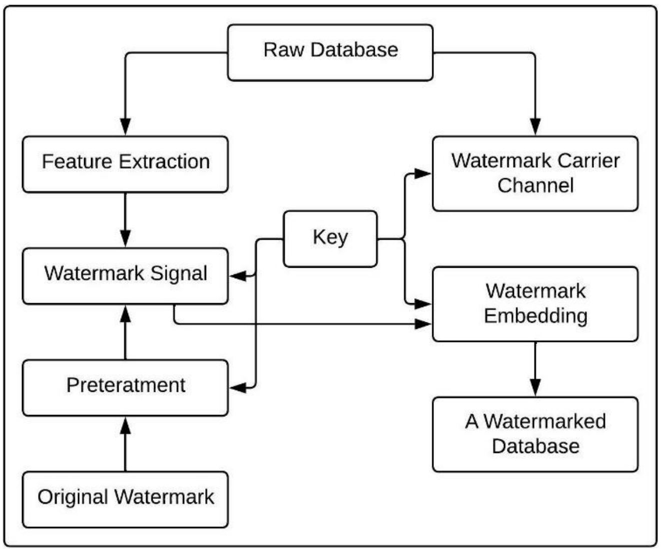


Figure 1. Database watermark generation and embedding process.

In most cases, the original database is not required to participate in the database detection process. The detection and extraction of watermark signals can be used to create a database for copyright certification and integrity verification. Additionally, you can track the location of data tampering and piracy. Pre-processing the watermark signal can yield data owner information if the watermark contains it. It is possible to make the watermarking hidden algorithm used in the database watermarking system available to the public. The security of the system is based on the key, and the key controls watermark production, transformation processing, watermark carrier channel acquisition, watermark embedding, detection and extraction, and other similar operations. Figure 2 depicts the detection and extraction of watermarks.

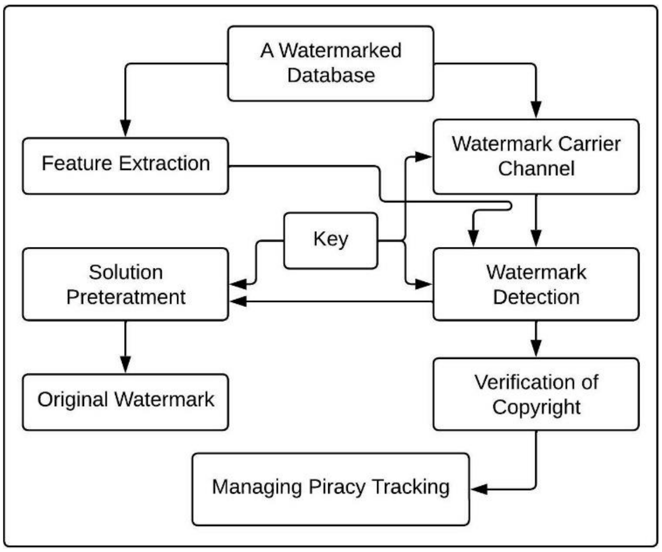


Figure 2. Database watermark detection and extraction.

The process of database watermarking consists of many essential algorithmic processes, each of which has a substantial influence on the performance of the database watermark [6]. Several different algorithms are used, some of which are watermark signal creation, watermark carrier channel acquisition, relationship, tuple tag, watermark embedding, and watermark detection and extraction. These complete steps are the foundation of the entire database model.

B. *Need of Database Watermarking*

Advanced watermarks are one of the different techniques which ought to assist with making the dissemination of advanced-material safer [7]. A qualification can be made between dynamic and inactive procedures:

- Active strategies, like cryptography, straightforwardly forestall unapproved conveyance of information; and
- Passive strategies, like advanced watermarks, serve more as a technique to give verification of possession freedoms.

Unapproved taping, perusing, controlling, or eliminating of information could prompt monetary misfortune or legitimate issues for makers and makers. Hence, architects, makers, and distributors of computerized information like pictures, recordings, sound sources, or interactive media material (for model, games, or virtual conditions) need specialized answers for manage the issues related with copyright assurance of their information.

C. *Properties of Database Watermarking*

Robustness depicts whether the watermark can be dependably identified after media tasks, design transformation, revolution, scaling or editing. It implies protection from fabricate, non-designated changes or normal media activities.

Security portrays whether the installed watermarking data can be taken out past dependable location by designated assaults. All watermarks aside from explanation ought to give high security.

Invertibility portrays the chance of separating the watermark after implanting it to re-establish the beginning. For instance, trustworthiness watermarks frequently need to check a record's uprightness and re-establish the first for clinical pictures.

Transparency connects with the properties of the human tactile framework. A straightforward watermark causes no relics or quality misfortune.

Complexity portrays the work and time expected to implant and recover a watermark. This boundary is fundamental assuming that we have continuous applications. Another viewpoint tends to whether the first information is expected in the recovery cycle.

Capacity depicts the number of data pieces can be implanted. It additionally addresses the chance of implanting numerous watermarks in a single report in equal.

Verification depicts whether it has a confidential confirmation, like private key capabilities, or a public confirmation, like the public-key calculations in cryptography.

D. *Limitations of Database Watermarking*

Watermarking depends on a secret key, which fills in as a transporter regulated to ship a message and insert it in the first satisfied [7]. The disadvantage is that knowing the secret key suggests the capacity of adjusting or eliminating the watermark which makes a public watermarking plan infeasible for the not-so-distant future. This implies that major improvements in copyright innovation will be situated close to the freedoms of the individual yet bar the data requests of the overall population.

V. PROPOSED METHOD

These days, the improvement of computerized innovation quickly increments and causes numerous duplications' or change of information like text, picture, sound, or video. In advanced framework, duplication of information can produce new information that nearly seem to be the first information. The proposed system as displayed in Figure 3 is to stay away from the control and duplication of information for the information base security the database management system.

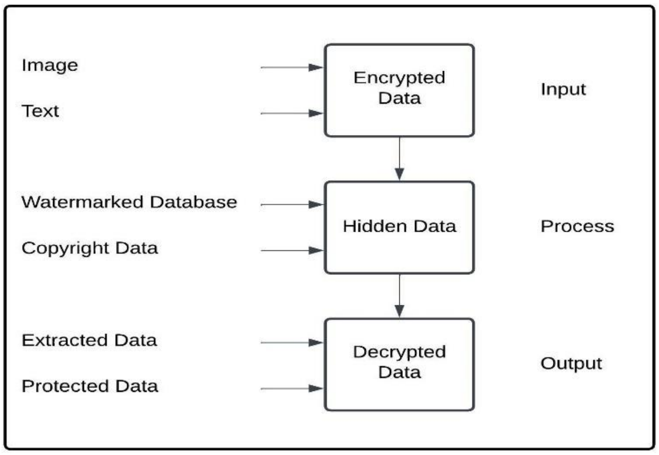
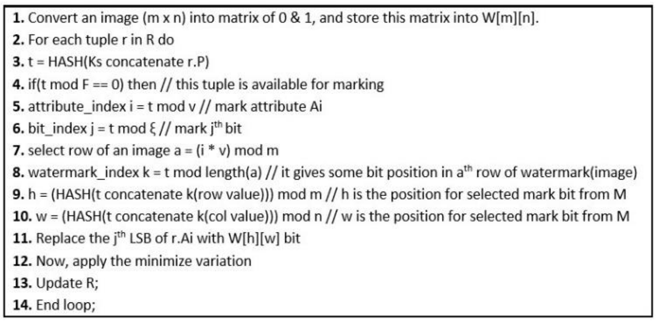


Figure 3. Proposed Data Ownership Protection via DBMS

The point of this strategy is to safeguard the responsibility for information with execution of watermarking into data set. A picture and text will be embedded into the traits of data set in double structure. Then, at that point, the undetectable watermark picture will be implanted with information for copyright reason. The information will be scrambled also, concealed in the framework. From that point onward, the encoded information will be put away and handled. Consequently, the client should insert the information with letter set and mathematical characters of mystery key. The extraction of information will happen after confirming the responsibility for relate information. Client should give exact data with the goal that the framework will unscramble the information for access control. The inclusion of watermark won't annihilate the unique data of the data set. Watermarking procedures can be applied by client itself when they give their information to a framework. The encryption technique will perform by making the watermark calculation before the installing system. We will embed a watermark data into the first information base and return checked [2]. This strategy won't ever change the privacy and honesty of the first data. Besides, carrying out mixed media watermark is simple for enormous trait set of information where it can work on the security of information.



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

Figure 4. Watermark Algorithm [2]

VI. DISCUSSION

In this review, the proposed procedure can be viable for future attempts to make a data set security system with new methodologies. Even though, watermarking strategies is broadly used to shield sight and sound information from control and duplication of soundtracks, recordings, and photographs. Presently, mixed media information additionally put away in data set administration framework. Various sorts of watermarking give different degree of security. It relies upon the critical place of these information. Client can get the advantages on the off chance that the processing framework isn't costly where it is planned with appropriate system. Other than that, picture-based watermarking method was proposed on the grounds that the picture will be supplement and switch over completely to be mixed picture in the principal stage. Watermarking is for the most part zeroed in on possession because of the information handling level where a portion of the watermark will be eliminated or erase by unapproved party. Additionally, installed watermark can be utilized for bio-metric sweep of the substance proprietor only, it can keep from any appropriation without the proprietor's anxiety. In this case, the proprietor is qualified to guarantee for content copyright's assurance on the off chance that the data set framework has security strategy. Watermark likewise choose recognizing controlled or any changed information. It is relevant to guarantee the uprightness of information is check through the trustworthiness of removed information. At the point at the point when data set substance is used for especially fundamental applications, for instance, business trades or restorative applications, it is fundamental for ensure that the data is given by right source without control. This can be achieved by embedding a watermark in the key data of the data set. Overall terms, there are two kinds of watermarking strategies which is watermark installing and water confirmation. The main stage is implanting technique where the mystery key is embedded into data set what's more, unreservedly open without getting to control. Implanting the information utilizing watermark technique can't be applied without precise figuring and computation. The subsequent stage is confirming the power of the substance where the client is expected to embed the precise mystery key to remove the information from the data set. The strength of the watermarking method is tried by different malignant assaults.

VII. CONCLUSION

Specifically, the research focused on the types of methods that can be used to increase the security level of a database management system (DBMS). The proposed method is to measure the secrecy of information is successful or not utilizing this methodology. The commitments of the method are the client can have a gotten information without changes and duplication. In expansion to, the calculation strategy is utilized by numerous information managers being developed interaction. In addition, watermarking approach can be applied in distributed computing administrations for high-security component in almost future. It is a to Identify methods for proprietorship insurance significant and testing task. The proposed method can be assessed utilizing data set trial test.

VIII. REFERENCES

[1] T.D. Vale, “Principles of Security and Integrity of Databases,” 15, pp. 401-405, 2014.

[2] U.P. Rao, D.R. Patel, and P.M. Vikani, “Relational Database Watermarking for Ownership Protection,” Procedia, 6, pp. 988-995 Technology, 2012.

[3] M. Şerban, “Methods to Increase Search Performance for Encrypted Databases,” Procedia Economics and Finance, 3, pp. 1063-1068 (2012)

[4] N. Vurukonda and B.T. Rao, “A Study on Data Storage Security Issues in Cloud,” Computing. Procedia Computer Science, 92, pp. 128-135, 2016.

[5] D. Trivedi, P. Zavarsky, and S. Butakov, “Enhancing Relational Database Security by Metadata Segregation,” Procedia Computer Science, 94, pp. 453-458, 2016.

[6] Cao, Z., Shi, G. and Wu, Q., 2019. Research on database watermarking based on Independent Component Analysis and multiple rolling. International Journal of Distributed Sensor Networks, 15(4), p.1550147719841004.

[7] Natarajan M, Makhdumi G. Safeguarding the digital contents: Digital watermarking. DESIDOC Journal of Library & Information Technology. 2009 May 1;29(3):29.

[8] Pan N, Wu X, Chi YL, et al. Acoustical diagnosis for gear box combined failures based on frequency domain blind deconvolution. J Vib Shock 2013; 32(7): 154–158.

[9] Wang Y, See J, Oh YH, et al. Effective recognition of facial micro-expressions with video motion magnification. Multimed Tools Appl 2017; 76: 21665–21690.

Cite this article as :

Saikat Baul, Md. Ratan Rana, "Analyzing Database Security and A Study of Ownership Protection using Watermarking Algorithm", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 208-216, November-December 2022. Available at doi : https://doi.org/10.32628/CSEIT228620
Journal URL : https://ijsrcseit.com/CSEIT228620