Review

Computation

Security Issues in Distributed Database Management Systems
Challenges and Opportunities

Anubha Pathak,* Sameer Saxena
AIIT, Amity University Rajasthan, Jaipur, India
*: All correspondence should be sent to: Anubha Pathak.
Authors' Contact: Anubha Pathak, E-mail: anubhapathak17@gmail.com; Sameer Saxena, E-mail: sameer.saxena4@gmail.com
DOI: https://doi.org/10.15354/si.23.re661
Funding: No funding source declared.
COI: The authors declare no competing interest.

Database management systems (DBMS) are essential systems of software technologies for multi-level and multi-angled operations with the utmost security. Currently, its form of distributed database (DDB) is very useful and popular in communication networks. The current write-up is aimed at investigating important security aspects and issues, exploring some major challenges pertinent to the security of DDB, finding solutions to the same, and eventually talking about some future opportunities through promoting research towards curbing these security-related points. To accomplish these tasks, the author has reviewed some of the latest and most pertinent research articles of the last ten years. It comprises the application of DDBMS, major pertinent issues within its range of investigation, and a conclusion.

Keywords: DDBMS; Security; Encryption; Authentication; Authorization; Multi-Level Access Control

Science Insights, 2023 August 31; Vol. 43, No. 2, pp.1019-1024.

Introduction

A DBMS is a type of transparent software to be used in creation, maintenance, and in imparting a well-controlled link to the various databases of the users. This is a pivotal technology required in all areas of service, e.g., industries, healthcare, aviation services, banking systems, etc. It provides a diversity of tremendous applications in scientific, industrial, and commercial domains. A distributed database (DDB) is a reasonable database capable of spreading on several computers in various locations at the same time and staying connected by a complex network of data communications. Today, the DDB is considered a unique and fundamental corporate resource for providing flexibility with wide applications.

In DDB, the network must permit sharing data with users at different locations. Its sites of distribution could spread over a large or small area, and computers may also range from large-scale computers to even supercomputers. The DDB requires multiple database management systems running at each remote site (1). Nowadays, various business conditions encourage the application of DDB, including the distribution and autonomy of business units, data sharing, data communication costs and reliability, multiple application vendor environments, database recovery, and the satisfying of both transactions and analytical processing. Today, though the DDB has advanced, it is still searching for its place in commercial markets due to security-related threats that are creating barricades in its secure functioning.

Database Security and Its Significance in DDB

It implies a group of complex measures (e.g., tools, techniques,

procedures, etc.) to be used for all-round protection, safety, and security of the internal database, its management, intrusion from external sources, invalid and illegal use, threats, and invasion of available or potential malicious software and cyber sites. Such security also includes the protection of the server of the database and the applications of other database workflows. Currently, the major issues of security are authentication, authorization, encryption, and implementing appropriate multi-level control to access the database pertaining to DDB. The security issues occur while using multifactorial control, testing capacity and load on the database, ensuring its endurance to user overload and distributed denial of service (DDoS), providing regular physical security (through security protocols and keeping multiple copies for emergency recovery), conducting reviews of the existing system for vulnerabilities and providing a plan to address them, and encrypting data for surplus security and confidential data.

Indeed, implementing database security is an essential support for any organization for several reasons, e. g., protecting against breaches of data for continuity of business and loss of intellectual property, preventing financial loss or minimizing financial damage, protecting the reputation of the brand for the customer base, and refraining from potential penalties and fines (2).

Hence, failure to ensure adequate enforcement and implementation of database security necessarily gives rise to deadly and detrimental challenges to confidentiality, integrity, reliability, and recovery of databases. These challenges are required to be addressed to pave the way for DDB's enduring functions. The present article includes major challenges and difficulties with the current DDB management system (DDBMS). For this purpose, the author has reviewed relevant research papers published or available online in the last ten years. At last, the author would suggest some measures for sorting out the challenges and showing silver linings for future opportunities.

Review of Literature: Major Security Issues of the DDBMS

The security of DDB is aimed at protecting data from malicious external cyber sources. As mentioned above, there are four components related to DDBMS security described below (3) (**Table 1**),

Authentication

This refers to the user providing a correct password in order to prevent any unauthorized access while establishing a connection. The user and password are created simultaneously and can be changed at any time. Passwords are assigned when a user is created. The user can change their password at any time (4). The password is stored in a data dictionary in an encrypted format to be known and understood only by the user. Authentication contributes significantly to DDBMS's security issues.

Various access control mechanisms deal with managing the access rights of users, as different users have different access rights to different databases. This is a basic technique for DDBMS security issues. In fact, a two-step authentication procedure is essential for the security of a database (5). Otherwise, it is highly likely for attackers to access a database with weak authentication and use techniques of brute force, social engineering, and direct credentials to identify and steal legitimate databases (6, 7).

Authorization

It aims at providing a secured access point to users for accessing authorized resources once at a time.

Encryption

A kind of encoding of data that can be understood only by the user Some good and useful qualities of standard encryption algorithms are Ron Rivest, Adi Shamir, and Leonard Adleman (RSA), the Data Encryption Standard (DES), Pretty Good Privacy (PGP), etc.

Multi-Level Access Control

It refrains the user from accessing the entire data but rather permits access to relevant information only. The access policies for multi-level systems are of two types: open (keeping all the data unclassified unless access to a particular type of data is conspicuously prohibited) and closed (access to all data is prohibited unless the user has the right and privilege to access specific data).

Major Challenges to the Security of DDBMS

There are some major threats to databases that are relevant to the security issues of DDBMS (8) and related to both states of data protection in databases: data at rest and data traveling. There are,

Excessive Privileges

It has various forms like excessive privilege abuse, legitimate privilege abuse, and unused privilege abuse. The user is likely to abuse privileges for an unauthorized objective. All these threats tend to cause potential damage by misusing data and creating a high risk to its security for two valid reasons: More than 80% of such attacks are executed by the company's employees and ex-employees, who enjoy a huge number of privileges in executing their wrongdoings with vested interests. It puts the database at stake. It is possible to curb these privileges through a strong control policy and a timely and good audit of privileges.

SQL Injections

It aims at undermining the original intent by submitting attacker-supplied SQL statements directly to the backend database. It has two types: SQL injection (for traditional databases by inserting unauthorized statements into the inputs) and NoSQL injection (for big databases by inserting malicious statements into big data components, e.g., Hive, MapReduce, etc.). Its measures of curbing are using stored procedures in place of implementing direct queries,

Malware

Cyber and network criminals, other sponsored hackers, and spies use advanced attacking and hacking software to silently enter the networks of companies to steal confidential and sensitive data. These malwares can be encountered by enabling firewalls and installing antivirus.

Weak Audit

Table 1. Comparative Analysis.

S.No	Name	Area of Research	Year	Advantage /Disadvantage
1	Rohilla S. and Mittal PK (2)	Data security: threats and challenges	2013	Temporary solutions to threats, e. g., confidentiality, reliability
2	Radhakrishnan S. and Akila A. (3)	Security issues in distributed database systems	2017	Multimodality and tools have been described, but all users don't know how to handle them.
3	Kumar CS, Seetha J, and Vinotha SR (4)	Security implications of distributed database management system models	2012	Talks about relational and object-oriented security issues, but no proper solutions are provided.
4	Soni D. N. Data Security (10)	Threats and security techniques	2015	Considerations for preventing sensitive data from being accessed by attackers
5	Rana S. et al. (14)	Distributed Database Problems	2018	Discussion about the dearth of security issues on DDBMS

Such audit policies and related technologies invite risks of compliance, deterrence, detection, forensics, and recovery. For example, failure to automate the recording of database transactions and conduct a proper audit may be risky at several levels in an organization.

Eventually, it may cause the company to be convicted on legal regulation issues. Such issues can be addressed by applying network-based audit tools.

Backup Exposure

It is commonly found that backup storage media is not often safe from external attack and could be the victim of several breaches of security measures in a database. In addition, negligence, and failure to properly monitor the activities of administrators with weak access to sensitive databases could also be devastatingly at stake. It can be protected by using encrypted databases for audits and controlled access to confidential data.

Weak Authentication

It supports the attackers and hackers to surmise the identity of authentic users of the database through techniques, e. g., brute force attacks, social engineering, etc. The two-factor authentication and password implementation could be helpful in shielding such security-related challenges.

DB Vulnerabilities and Misconfiguration

In fact, it is easy for attackers to find default accounts and configuration parameters for exploiting companies and organizations. But organizations often struggle to protect databases despite the availability of patches for several reasons, e.g., high workload and mounting pending backlogs of the same, complex, and time-consuming tests of patches, and challenges in finding a maintenance window. It is possible to curb these issues by permitting "no default accounts" and using a new username or password every time.

Unmanaged Sensitive Data

This is common in many companies, and they forget confidential parts of databases to manage, causing a new database that is highly likely to be invisible to the security team and measures. Such data can be protected through encryption of sensitive data, applying required control and permissions to the database, consolidating or hardening TCP/IP by appropriate setting of the registry, using a network intrusion detection system (IDS), etc.

Limited Security Expertise and Education

This is considered under non-technical security issues, which often are not compatible with data growth due to a lack of expertise to implement necessary security controls, policies, conduct incident response processes, etc. Proper, updated, and adequate awareness, knowledge, and experience of staff are necessary.

Some Security Measures and Control Methods

Creating Threats and Challenging DDBMS (9, 10)

Access Control

In order to avoid data breaches in database systems, it is a mechanism that permits creating, editing, reading, and deleting files on file servers (11) only to authorized groups and restricts access to unauthorized individuals. The primary reason a business has to implement data access control is for data security (12). However, in the field of data engineering, it poses a long-term security concern due to the difficulty and complexity of authorizing individuals to access data. When data engineers choose to provide broad permissions, access cannot be revoked when it is no longer required. Therefore, security risk is a long-term responsibility that data engineers must bear.

Encryption and Authentication (13)

To safeguard the contents of database data, encryption uses a key approach in which plain text is changed into cipher text with the use of a key. We may then use the same key to decrypt the data for the legitimate user. Authentication: In this procedure,

the username or any other password-like key used to decode the encrypted data is utilized to identify the user.

Inference User Policy Identification (14)

The goal of the inference strategy is to stop hackers from getting access to data. Data is protected to a certain extent. Users must first be recognized by the database and given access permission before they may access the resources. This is necessary for the security of the database. The illegal user, however, may employ several strategies, such as using the default password, avoiding authentication, etc. The private communication level can be used to implement users' identification. The illegal consumer, however, may be able to use various techniques, such as using the default password, avoiding confirmation, etc.

Program Permissions and Data Rights

This is the right to execute, retrieve, or update information in a program on an application server or database.

Inference Policy

It aims at preventing the indirect reveal of data in any of three ways of unauthorized disclosure of data: (i) correlated data, when visible data are semantically related to invisible ones; (ii) missing data, containing null values masking confidential data; and (iii) statistical inference, providing statistical information about entities.

Accountability

This is the process of maintaining an audit trail for user action on the system and auditing, monitoring, and keeping records of the configured database. To protect the actual condition of the data, which requires established access to the databases, accountability and audit checks are necessary. These are controlled by auditing and records. Access efforts and their status should be documented in the audit record files whenever a user gets to authenticate successfully and tries to access a resource. Both their successful and unsuccessful attempts ought to be documented by the system.

Some Unique Challenges to DDBMS

Problems Related to Centralized or Decentralized Approval

In developing DDB, there are two levels or types of granting access to the system for the user,

- Granting Access to the System at Home Location

Relatively, it is easy and secure to handle, and its success depends on reliable and valid communication between various locations. Since different locations are granted access, the chance of an increase in unauthorized access is high. This is because the entire system would be compromised if a single location was given unauthorized access. On the contrary, the chance of compromise due to unauthorized access would be less if access control for all users could be maintained at each location.

- Granting Access to the System from the Remote Location of the User

In this type of access, it is important for the remote location to get all essential authorized information. Despite claiming more security, this technique has major disadvantages, e. g., the requirement of additional processing overhead (especially when such processes require the participation of several locations), the expensive maintenance of replicated clearance tables of passwords, and the risk of stealing (despite being encrypted).

Proposed Solutions to the Aforementioned Challenges of DDBMS

There are some of the latest and still emerging tools of security for DDBMS, which are as follows,

- Data warehouses, along with data mining systems, collaborative computing systems, distributed object systems, and the web, use avoidance and detection algorithms in deadlock management (15).
- The tool of the data warehouse facilitates a suitable technique of control on data access and duly ascertains the maintenance of security in constructing a warehouse of data from the supported systems of the database, e.g., integration of policies for the warehouse's security, audit of the warehouse from time to time, security of retrieval of data, etc.
- Data mining is useful in retrieval-related security by providing a retrieval controller to the warehouse of data and preventing murky motives by the user.
- The retrieval controller works between the data mining tool and the database, which is controlled by a DBMS. Other tools and techniques, like collaborative computing systems, distributed object management systems, and the web, provide security to databases, operating systems, web servers, web applications, clients, and networks.
- Deadlock management is required when users block the resource database while the same is requested by other users at different locations. At last, data fragmentation could also be a good option, which provides a full or fragmented copy of the database for users at different sites (16). However, it has high temporal complexity and low referential integrity in DDBMS.

Conclusion and Opportunities

The investigation of the major challenges of DDBMS explored some opportunities for discovery and invention that could be highly useful in intervening in its security-related challenges. Firstly, problems related to the inference of retrieval from a data warehouse are an essential domain requiring a high level of research to find out techniques and tools for controlling such issues. Nonetheless, we should not forget that human errors are also likely in formulating policies and developing techniques for enhancing security in warehouses of data, and, as a consequence, minor mistakes and negligence could cause a great and irreparable loss. In this context, lack of updated technical skills multiplying with inadequate professional experience is a big issue in advanced research and implementation of novel techniques, e.g., application of query processing in geographically separated databases for minimizing communication and processing costs (17).

Secondly, there are issues related to data mining and replication control (RC) (18) that need intervention. In fact, data mining is not sufficient for securing sensitive information from unclassified information, which, in turn, is highly likely to cause problems with the retrieval of databases. Effective innovation in the replication control is required in DDB, which (i.e., RC) is used when the entire or some percentage of the database is required to be copied at various geographically dissimilar sites. In addition, in a similar vein, it should be kept in mind that it is impossible to cover all plausible ways of retrieval-related challenges through data mining despite the fact that the user could be applying only one tool at one point in time; however, they may have several tools available at the same time. Thus, a highly qualified controller of retrieval in data mining is required to be discovered through research, which is likely to open a huge domain of professional opportunities in detecting and identifying all tools of the user being used with some illegitimate interests and intentions.

Third, since all anti-virus programs are not equally effective for the long term when subscribed once, they need to be regularly updated, effectively functional for a long time, and essentially cost-effective. Furthermore, pertinent scientific research may curb the application of pirated versions of most of the anti-virus programs, which are cheaply available but highly risky for losing sensitive data. Similarly, a temporal test of the effectiveness of the network-based audit tool must be conducted and essentially renovated. Misconfiguration-related problems and difficulties can be sorted out by special training, developing less time-consuming tests of patches, work-distribution or rotation-basis assignment among staff, appointing or hiring experts, etc. Manpower could be developed for training staff with updated knowledge and technical skills for those with limited education and technical expertise.■

References

1. Shine on: Database Security. Last accessible date: March 31, 2022. Available at: https://www.techopedia.com/definition/29841/database-security
2. Rohilla S, Mittal PK. Data security: Threats and challenges. Int J Adv Res Comput Sci Softw Engin 2013; 3(5). Available at: https://www.api.semanticscholar.org/CorpusID:112248228
3. Radhakrishnan S, Akila A. Security issues in distributed database system. Int J Adv Res Comput Sci Softw Engin 2017; 4(7):301-304. Available at: https://www.researchgate.net/publication/325737373_Security_Issues_in_Distributed_Database_System
4. Kumar CS, Seetha J, Vinotha SR. Security implications of distributed database management system models. Int J Adv Res Comput Sci Softw Engin 2012; 2(11):20-28. DOI: https://doi.org/10.7321/jscse.v2.n11.3
5. Ali A. Afzal M M. Database security: Threats and solutions. Int J Engin Invent 2017; 6(2):25-27.
6. Singh S. Kumar RR. A review report on security threats on database. Int J Comput Sci Inform Technol 2014; 2014:3215-3219. Available at: https://api.semanticscholar.org/CorpusID:15569165
7. Jain S, Chawla D. A relative study on database security threats and their security techniques. Int J Innov Sci Res Technol 2020; 5(1):794-799. DOI: https://doi.org/10.13140/RG.2.2.11657.60000
8. Malik M, Patel T. Database security- attacks and control methods. Int J Infor Sci Techn 2016; 6(1-2):175-183. DOI: https://doi.org/10.5121/ijist.2016.6218
9. Sah MK, Kumar V, Tiwari A. Security and concurrency control in distributed database system. Int J Sci Res Manag 2014; 2(12):1839-1845. Available at: https://api.semanticscholar.org/CorpusID:212577605
10. Soni D N. Data security: Threats and security techniques. Int J Adv Res Comp Sci Softw Engin 2015; 5(5):621-624. Available at: https://api.semanticscholar.org/Corpus ID:112523027
11. Guide: Access Control. Web page as it appeared on 10/08/2023 (the last time our crawler visited it) Available at: https://satoricyber.com/access-control/access-control-101-a-comprehensive-guide-to-database-access-control/
12. Singh P. Kaur K. “Database security using encryption,” 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 353-358, DOI: https://doi.org/10.1109/ABLAZE.2015.7155019
13. Gahlot S, Verma B, Anurag Khandelwal, Dayanand, 2017, Database Security: Attacks, Threats and Control Methods. Int J Engin Res Technol 2017; 5(10).
14. Teimoor A R. Database security concepts, threats and challenges. June 2018; DOI: https://doi.org/10.13140/RG.2.2.34426.75203
15. Hiremath DS, Kishor SB. Distributed Database Problem areas and Approaches. J Comp Engin: National Conference on Recent Trends in Computer Science and Information Technology 2016; 2016:2278-8727.
16. Ezechiel KK, Shrikant, Agrawal R. A systematic review on distributed databases system and their techniques. J Theor Appl Infor Technol 2019; 96(1).
17. Boicea A, Radulescu F, Truica CO, Urse L. Improving Query Performance in Distributed Database. J Contr

Engin Appl Infor 2016; Vol 18(2):57-64.

18. Rana S, Sohel MK, Arman S, Distributed Database Problems, Approaches and Solutions - A Study. Int J Mach Learn Comput 2018; 8(5). DOI: https://doi.org/10.18178/ijmlc.2018.8.5.731

Received: June 26, 2023 | Revised: August 19, 2023 | Accepted: August 27, 2023