ISSN No:-2456-2165

Review on Database Models and Security Breach

[1]Abhilash B., [2]Amrutha M., [3]Charitha U. M., [4]Chiranth B. K., [5]D. Khasim Vali
Associate Professor, Vidyavardhaka College of Engineering
Mysuru, India

Abstract:- Nowadays, there is ample growth in data which is generated in discrete fields. The authoritative operations like updating, deleting, altering, etc. are handled using the database. The operations like alteration of data and its maintenance are fulfilled using the Database Management System. This method of storing data is an effortless and efficient way to manage it. By taking into consideration the value of data, it is truly essential to secure the assorted data present in the system. The data must be secured in such a way that, it has to reciprocate all types of possible database attacks. In order to provide security in such a manner, many types of security models which are in concern with different issues of the database security has to be designed. They might be different because of their various assumptions about what constitutes a secure database. So, it becomes very hectic for database security aspirants to select a pertinent model for securing their database. Securing database is an important approach for the routing of explicit and directive-based database security requirements. As the complexity of the database increases, it is likely to have security issues.

***Keywords**:- Database Models, Database Security Issues, Database User Privileges, Database Security Models, Privileges Exaltation.*

I. INTRODUCTION

A database can be defined as an assemblage of data that is saved on a computer system's hard drive. Databases allow all of its legitimate users to access its services to much possible extent providing multiple interfaces to the different levels or community of users. It can be viewed as a conglomeration of queries, tables, views, etc. By taking into consideration the security of the database, serious thought on designing a series of security procedures has to be made with the sole reason for monitoring the database indefinitely.

II. LITERATURE SURVEY

The brisk evolution and expansion of information technology have proposed many scopes for cohesive business actions. With the enhancement of technology, we can find hype in operations such as sales service, customer care, human resources, and production activities. [1]However, all these improvements have caused an emergence of various security issues. There are many examples of firms falling prey from this trouble making disputes. Besides, there are communities intended to target the security systems to get affected by their corruptive implants.

Privileges exaltation is another threat to the database. The latter will occur when there is a transformation of rights from normal user to administrator level by taking database platform software susceptibility. For instance, in a firm accounts section, an intruder would integrate his existing rights with that of superior privileges which is enough to make unlawful actions. It is achieved by employing software vulnerabilities in the database system.

There are several ways of how one can abuse the prerogatives of the database. The users might misuse their powers for nefarious activities. There are different flavors of privilege faults: Exorbitant privilege abuse, lawful privilege abuse, etc. The tragedy of these types of abuses is that the system gets depraved by trusted users [2].

There are varied reasons for which the granting of excessive permissions becomes an issue. A company's confidential data is usually affected relatively 80% by its employees/ex-employees. The investments of rights more than what a user deserves will create steep disputes.

Pernicious codes and other outbreaks are expanding in intensity and the devastation that is induced. Within no time, systems have to become more ardent in their security viewpoint. Reactive security [3] will not be employed anymore with the intervention of these disputes. Hence, organizations must be ready with what the forecoming trends, perils, and menace are, and thereby making the system more safe and secure.

The designation of security policies must be ahead of any exertion in such a way, so that future amendment and endorsement can be adequate and easily manageable. The security system must be compacting along with flexible for the end-user to make him complacent so that the latter doesn't feel that the policies revolve around him. Users who endure these policies and systems too prohibitive will be annoyed greatly by this.

In general, the data is delivered in a plain text which is not a secured way and grants an assailant (want to access the data) who has achieved entry to data paths in our network to "Listen In" or portray (read) the transit. The criterion wherein an intruder is overhearing the transmission is indicated as sniffing (Data modification) or snooping (IP Address snooping). A distributed attack needs an adversary to introduce code, such as a back-door program or Trojan horse, to the "credible" software that will be passed on to various firms and its users. Distribution attacks focus on the nasty modification and alteration of hardware or software at the time of disposal. These incursions inject malignant code such as a back door to the stock and will anonymously earn unauthorized access to information which is the same as losing the privacy of the data [4].

The initiative database system is subject to the prodigious class of hazards. The users having access rights which allow them to execute other tasks not comprised in their job will discover harmful intent thus pointing to squander of such allowances. As an outcome, all users who carry out various tasks are provided with a default degree of privileges that handout access in excess. [5] A timely and proper recording of database transactions are assured by the database audit policy. Such a protocol must be a part and parcel of the database security scrutiny as all the delicate database transactions have a mechanized record and the absence of which imposes a severe hazard to the organization's databases.

Surveillance is considered to be a unilateral problem for any security-relevant products. A system entity should be protected from any malignant attacker from outside. A system is considered to be secured when it cannot be attacked and diverged along its normal operational flow from the outside intruder who retains definite potentials. One such example is that important data cannot be extracted from these external intruders [6].

The record of graphs collection is related with pointers which are how the data in any network data model is organized. The address of further records located on the disk is determined by the pointers which are the physical address. A Network data model is more versatile than a hierarchical data model and efficient navigation will be supported [7]. Based on the object-oriented programming (OOP) the data model is designed. In the object-oriented database, an object is the basic and a run time entity with its private and exclusive states.

The NoSQL database is distinguished from others by its storage resilience and data manipulations, performance improvements and allowing for effortless scalability [8].various kinds of these NoSQL databases can be found today. Each of these kinds is suitable for different purposes. Some of such example include Mongo DB, Disney, bit.ly, source forge, CERN, etc.

Over the last decade, all the necessities and wants of database management systems (DBMS) have evolved considerably. The relational model (Codd 70) was developed in the early 1970s for business applications as a data model. [9] The drawback of this model is its restricted outspoken power to gestate the real world of business applications. The Entity-Relationship (ER) is used as an environment for conventional applications (Chen 76) as a high-level conceptual model. Scientific applications cannot be effectively modeled by the tools which are alike to the ER model.

A biometric identification system is a twosegment system. The two segments are special hardware and processing hardware. The special hardware part comprises a sensor, which in turn is connected to the processing hardware. [10]The processing hardware does the job of recognition and identification, usually a PC. These different parts of the system are liable for a perilous threat to the security of the entire isolated secured system.

III. ANALYSIS

In order to make any changes to the existing system, we will have to first clearly analyze the locations of the system where we might find the flaws. Some of them are as follows:

➢ *Constant Intervention*

Database audit logs require daily review to make certain that there has been no misuse of the gathered data. This requires overseeing database allowances and then consistently amending the user access accounts.

➢ *Assorted Security Modes for Applications*

More often not all the applications developers will differ the scheme of security for different applications that are being utilized within the database.

➢ *Post-Upgrade Appraisal*

When a database is upgraded it is necessary for the administrator /designer to ensure that security is consistent across all programs by conducting a postupgrade evaluation.

➢ *Fissure the Position*

Sometimes organizations fail to split the duties between the IT administrator and the database security administrator. In this scenario, the IT administrator is expected to do the job of the security administrator.

➢ Application Bluffing/Spoofing

Hackers are capable of creating applications that feature the existing applications connected to the database.

IV. CONCLUSION

Based on the drawbacks of the current system, we can have slight changes in the access privileges provided on the database servers. One such observation is designed in figure 1. The normal flow of accession of the resources from the database could be altered slightly. In order to make sure that the data stored ends up with only the legitimate users, few steps of security procedures which are complex enough to break could be implemented. A key generation algorithm could be designed such that no intruder can predict the key, as for every trial/access for the server there will be a new random key generation. So that it is difficult to hack the keys or to even predict it. This could be used to feed the server in order to have access.

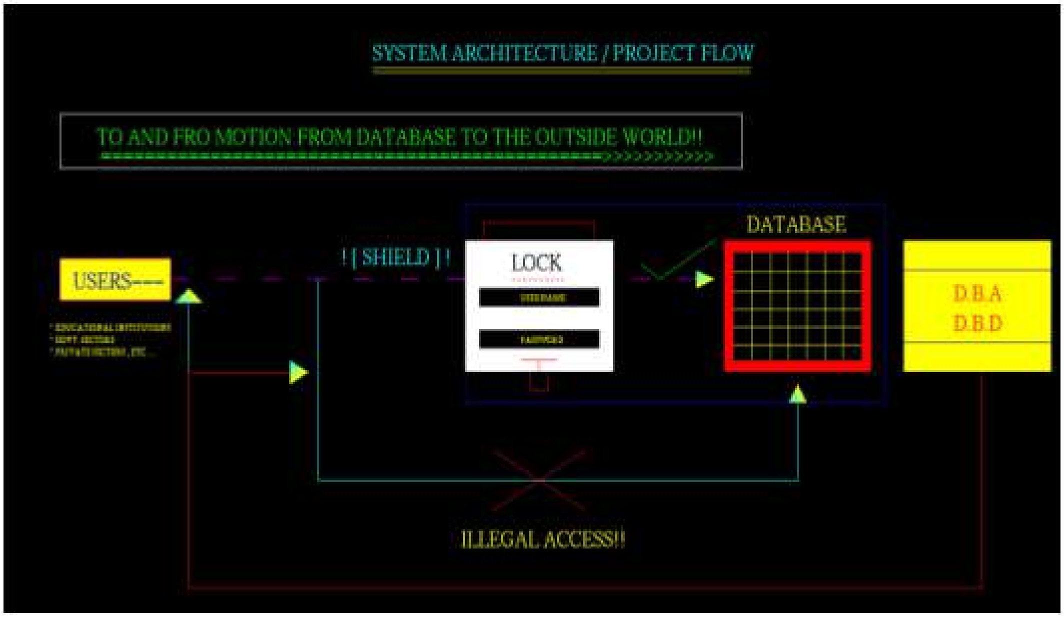

Fig 1:- Architecture of the proposed database security procedure and sequences.

REFERENCES

[1]. Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili, "Security in Database Systems", Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350 Volume 12, Issue 17, Version 1.0, 2012.

[2]. Mubina Malik and Trisha Patel, Samavi1, CMPICA, Charotar University of Science & Technology (CHARUSAT), Changa, "Database Security - attacks and control methods" International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016.

[3]. Shailja Pandey, Department of Information Technology, BBDNITM Uttar Pradesh Technical University, Lucknow, India. "Modern Network Security: Issues And Challenges", Shailja Pandey et al. / International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol. 3 No. 5 May 2011.

[4]. Shilpa Pareek, Ashutosh Gautam and Ratul Dey, Department of Computer Science And Engineering, University of Engineering & Management, Jaipur, India. "Different Type Network Security Threats And Solutions, A Review", ISSN 2321-5992, Volume 5, Issue 4, April 2017.

[5]. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar, "Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888), Volume 47– No.12, June 2012.

[6]. Ueli Maurer, Department of Computer Science, ETH Zurich CH-8092 Zurich, Switzerland. "The Role of Cryptography in Database Security", Copyright 2004 ACM 1-58113-859-8/04/06, SIGMOD 2004, June 13–18, 2004, Paris, France.

[7]. Dr. P. K. Rai, Prof. I/C, BCA & Head, Computer Centre APSU Rewa, and Pramod Singh Research Scholar, (M.P), Satna, India. "Studies and Analysis of Popular Database Models", International Journal of Computer Science and Mobile Computing, Pramod Singh et al, International Journal of Computer and Mobile Computing, Vol.4 Issue.5, May- 2015.

[8]. Innocent Mapanga, Amity University, Noida, Haryana, India & Prudence Kadebu, Harare Institute Of Technology, Harare, Zimbabwe. "Database Management Systems: A NoSQL Analysis", International Journal of Modern Communication Technologies & Research (IJMCTR).September 2013.

[9]. Y. Zhou, School of Geography, Clark University, Worcester, MA 01610, M.A. Gennert, N.I. Hachem, M.O. Ward, Computer Science Department, Worcester Polytechnic Institute, Worcester, MA 01609. "Requirements of a Database Management System for Global Change Studies".

[10]. Filip Orság, Martin Drahanský, BUT, Faculty of Information Technology, Department of Intelligent Systems, Božetěchova 2, CZ – 612 661 Brno, Czech Republic. "Biometric Security Systems: Fingerprint and Speech Technology", research-based, Ph.D. paper.

[11]. Suvasini Panigrahi, Shamik Sural, A.K. Majumdar, "Detection of intrusive activity in databases by combining multiple evidences and belief update", Computational Intelligence in Cyber Security 2009. CICS '09. IEEE Symposium on, pp. 83-90, 2009.

[12]. Elisa Bertino, "Data Security and Privacy: Concepts Approaches and Research Directions", Computer Software and Applications Conference (COMPSAC) 2016 IEEE 40th Annual, vol. 1, pp. 400-407, 2016.

[13]. Ghassan "Gus" Jabbour, Daniel A. Menasce, "The Insider Threat Security Architecture: A Framework for an Integrated Inseparable and Uninterrupted Self-Protection Mechanism", Computational Science and Engineering 2009. CSE '09. International Conference on, vol. 3, pp. 244-251, 2009.

[14]. Nedhal A. Al-Sayid, Dana Aldlaeen, "Database security threats: A survey study", Computer Science and Information Technology (CSIT) 2013 5th International Conference on, pp. 60-64, 2013.

[15]. Anam Zahid, Rahat Masood, Muhammad Awais Shibli, "Security of sharded NoSQL databases: A comparative analysis", Information Assurance and Cyber Security (CIACS) 2014 Conference on, pp. 1-8, 2014.