International Journal of Computer Engineering and Applications, Volume VI, Issue I April.14
www.ijcea.com ISSN 2321-3469

STRATEGIC FRAMEWORK OF MULTILAYER CHECKPOINT FOR DB SECURITY

Nooruldeen Nasih Qader
University of Sulaimani, Computer Science

ABSTRACT:

This paper proposes the strategic framework of Multilayer Checkpoints for Database Security (MLC-DBS), which will be undoubtedly highly beneficial for small database and big database because both sizes contain valuable data. All they need to implement this framework for any size of the database is deciding how many layers are required and what specific layer is more necessary. Thus, factors affect required layers to specific database are discussed because the disadvantage of MLC-DBS is the complexity, which leads to make an application not user friendly and costly and time consuming. One solution reduces layers unless it is necessary. A balance between security and simplicity is required since both are required.

There are many techniques of security, which differs from multi sides, reliability, requirement, cost, speed, policy… etc, which means, a technique may be the best for some place, whereas the same technique is totally insufficient for another place. MLC-DBS is the flexible solution, and systems that protected by MLC-DBS are more secure than others, because, if one or some of the checkpoints are cracked, there are other that remains the system in secure.

Keywords: Database, security, encryption, intrusion, authentication, NOSQL, notification system

[I] INTRODUCTION

Database (DB) considers significant applications of computer science. The reason behind this fact is the tremendous influence of DB on modern daily life. Therefore, DB almost forms an important part of any Information system application. On the other hand DB starts from the beginning of modern computer and it continues developing. DB security is a specialist subject within the area of Information security . Since sensitive data stored in DB, DB security considers one of the main issues in this field. DB and DB technologies form a core component of many computing systems and applications which allow data to be stored, retained and shared electronically. As the use of DB systems and the amount of data contained in these systems grows continuously and exponentially, DB security has become an issue of utmost importance due to an increase in the number of incidents reporting the unauthorized exposure of sensitive data. Therefore, the DBs should be protected in such a way as to restrict the unauthorized persons from accessing the sensitive contents of the DB as well as the overall DB as a whole. Thus, this paper proposes a strategic framework that contains various techniques, providing security to DBs.

Having a security system is an essential target for any organization, for doing that, an excellent security policy should be designed carefully plus a multilayered approach associated with security considers among the best choices . While DB security has a wide variety of security topics as physical security, network security, authentication and encryption, this paper targets the concepts and mechanisms specific to the problem of securing the data. This paper discusses ways to protect the DBs concerning an array of methods and discusses a procedure which provides safety to DBs from unauthorized users. Thus, this paper involves various techniques, discussing a DB protection problem, which is securing the internal contents of the DB and methods to restrict the usage of the DB .

DB security involved with ensuring the secrecy, availability and integrity of data stored in a DB. The security styles for specific DB techniques typically specify further protection administration and management features alongside various business-driven information protection controls within the DB applications and features (e.g. data access validation and audit trails) .

Due to the significant role of DB security many models have been developed and it is still an open issue in both fields DB and information security. Multilevel security is one of this models, which involves the policies they can hold information at a number of different levels of classification (Confidential, Secret, Top Secret, . . .), have to ensure that data can only be read by a principal whose level is at least as high as the data's classification -.

Although applying the primary security mechanisms, the DB stills violate from both of external and internal users. So, the researchers create an Intrusion Detection System (IDS) to detect intrusion as it occurs and override its malicious affects soon . IDS proposed in the framework to support the DB security. IDS made sending notifications to the authorized user if any unauthorized user accessed or attempted to DB. Intrusion is only the unauthorized access of data it is known as intrusion. Data mining approaches could be used for IDS. IDS determines the normal transaction and abnormal transaction. Notification system is integrated with an IDS to send notifications to the authorized user via devices such as mobile phones. Figure 1 shows implementation of the MLC-DBS framework.

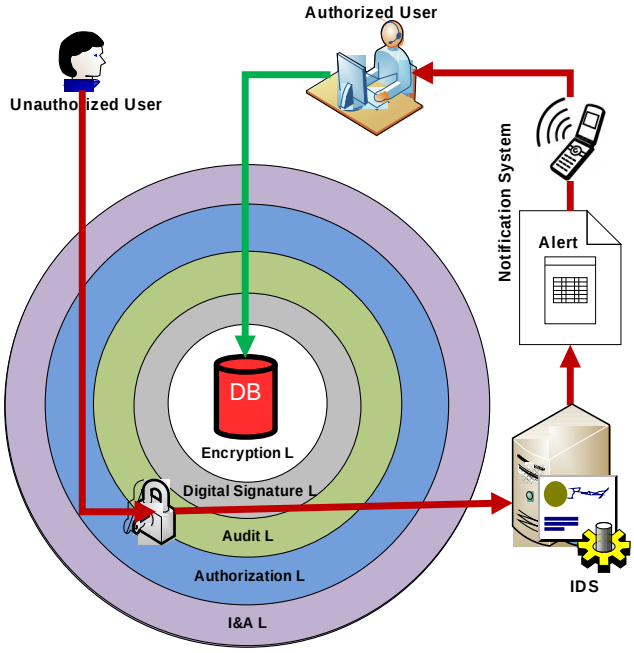

Fig: 1. MLC-DBS Framework

The rest of this paper is organized as follows: the significant role of DB security and the relation between DB sizes and security issue is discussed. Affects factors for selecting number of the required layers and type of layer for specific DB is presented, the goal is to protect DB from insider and outsider attacks. MLC-DBS diagram is presented followed by

conclusions and future works.

[II] THE AIMS AND PROBLEM STATEMENT

It is important to assume that any security system may be broken, however it is strong. On the other hand, because of the significant role of DB researchers should work to provide more security to DB. The main aim of this paper is designing a strategic framework for securing the DB system by using MLC-DBS, the established secure DB system should have reasonable complexity, and proposed secure system framework for DB with inexpensive cost.

[III] SIGNIFICANT ROLE OF DB SECURITY

Even before the existence of computers, we had learned and concentrated on the ways of learning and protecting their files and documents. Today, most of the documents are in the form of files and are saved in computers, while some other important data are usually located in the organization's DB, we wanted to make sure that they will practice security measures and ensure that all of their business files and data are kept secure - this is the reason why DB security services are usually being looked for, along with some security tools that could further help them keep their files and documents safe and secured at all times. Cybercriminals often target the DBs because that is where the money is. The DBs that power websites hold a great deal of profitable information for those who are looking to steal credit card information or personal identities .

DBs are used in various kinds of applications such as surveillances, record keepings in medical fields, military fields, storage of confidential documents in defense systems, crime related information in investigation fields, etc. These DBs are most vulnerable to unauthorized accesses by eavesdroppers with an intention of stealing the confidential data. Therefore, there is the need of restricting the access to the DB by unauthorized users, along with providing the security to the inner contents of the DB. The MLC-DBS framework can encapsulate the secret information in the DBs under multi protecting covers, that is, restricting access, securing the DB contents, intrusion detection, notification system, backup… etc.

Problems of DB security are coming from the fact that the DBs are extremely complex systems and difficult to configure and secure correctly. Most DB administrators (DBA) have a full time job administering the complexities of these systems. As a result serious security vulnerabilities and misconfigurations frequently go unchecked or completely undetected. The traditional security communities have mostly ignored the topic of DB security. DB professionals usually do not consider security as one of their primary responsibilities. DBAs are judged more by how fast the DB runs than how secure it is. Today, one would need an army of administrators, which they support with the sophisticated knowledge both in the technical issues and in the policies that are to be enforced. Since such administrators are costly and scarce, little is done .

Computer securing often get more emphasis than securing DB. Application and/or DB level security cannot solely protect data (e.g. disallow update access to the salary table to Fred does not provide any security if Fred can modify the data on the disk directly, or steals the disks and use a binary editor). DB security cannot be seen as an isolated problem because it is affected by other

components of a computerized system as well, so it must be used in conjunction with other layers of security including operating system (OS) security, network security and application security.

E-commerce applications have become popular daily because they are working just like a virtual store. Today's distributed e-commerce applications trust various technologies within their realization typically, including the Internet, scripting languages, server-part digesting and an underlying DB. The mix of these systems creates something that requires focus on the security problems of every component. Therefore, security aspects linked to authentication, authorization, and transaction DB carefully have to be managed. Clearly, the web transaction requires customers to disclose a great deal of sensitive private information to the suppliers, placing themselves at substantial risk. Understanding (indeed, actually precisely defining) consumer trust is vital for the continuing advancement of e-commerce .

[IV] SMALL DB VS. BIG DB

Whenever we discuss DB protection, we begin by discussing extensive DBs maintained simply by large businesses usually. But it could be argued that biggest DB challenges of most are those confronted by the small businesses, which are struggling to get a basic security set up just. Today the business environment in which smaller businesses are operating, dictates that new needs have to be applied in small sized businesses to improve their DB protection. They ought to adopt a new group of security equipment, which require simple installation, maintenance and use. Security equipment's protect the small company DBs from DB protection breaches .

In both cases, instead of going for the costly DB servers which additionally requires extra hardware as well as the extra expenses in training and handling, the flat file may be considered as a candidate due to its easy handling nature, fast accessing, and of course free of cost. But the main hurdle is the security aspect which are not up to the optimum level .

Although large companies are the targets of data breaches by hackers often, small businesses have to be more worried about their DB security also. In fact, small businesses also have much more to lose because of data breaches since they generally have fewer infrastructures set up with less IT personnel, so the threat of data loss is a lot higher in comparison to large companies. Although small businesses do not utilize the same security steps that large companies do, there are many other security measures by which your small business can reinforce its DB security .

The strategy framework proposed by this paper will undoubtedly be highly beneficial for small DB and big DB because both sizes may contain valuable data. All they need to implement the framework for any size of the DB is deciding how many layers is required and what specific layer is more necessary.

[V] REQUIRED LAYERED TO ENSURE DB SECURITY

The idea of MLC-DBS is, if one or some of security layers are cracked, there are other layers remain information secure, but the disadvantage of MLC-DBS is the complexity, which leads to make an application not user friendly and costly and time consuming in design and maintenance

phase. So a balance between security and simplicity (or transparency) is required since both are required.

MLC-DBS is an application to protect sensitive data, although DB has different vulnerabilities, still people have no choice to store their own data in DB systems, so the need to secure DB systems becomes an important issue. Different approaches adopted to secure DB. MLC-DBS system may be favored under specific circumstances.

How many layers are required to secure DB? This issue should be considered good because as adding any checkpoint layer increase security, it will increase cost and complexity. Therefore, many models have been designed for securing DB, but they are suffering from tradeoff between complexity and security. Complexity issue needs further consideration because DB and DBMS have their own complexities, this issue was the main factor behind the trend of NoSQL DB. Due to dependence on even more flexibility, that schema-free NoSQL DBs have grown to be so popular. Typically, designers do not need to specify a schema in advance. Moreover, adding a field to a data structure can be carried out and relaxed anytime. So, flexibility is the main advantage of a schema-less DB .

Increasing DB security is among the most effective and cost-effective steps a business can undertake to avoid data leaks. Though this is a complex setup, the security advantages are well worth your time and effort. Digital world keeps growing very fast and be more complicated in the quantity (terabyte to petabyte), range (structured and un-organized and hybrid), velocity (higher speed in development) in nature .

Factors affect required layers to specific DB are:

1. DB environment, i.e., is it online or offline? In the cloud or at the LAN? Expected DB user?
2. The value of DB, the sensitivity of data is it a secret or top secret?
3. The used DBMS and security features embedded and enabled in the DBMS.
4. Scalability of DB and is it SQL or NOSQL DB.
5. Expected nature of internal and external threads.
6. Vulnerabilities that needs urgent actions.

So, the understanding of environmental conditions, the design of security mechanism, and the policy are the cornerstone of information security. Thus a complete solution to data security must meet the following three requirements: 1. Secrecy or Confidentiality: Protection of data against unauthorized disclosure, 2. Integrity: Prevention of unauthorized and improper data modification, and 3. Availability: Prevention and recovery from hardware and software errors. These three requirements arise in all application environments .

[VI] ACCESS CONTROL

Like all tangible assets which have to be protected by an ongoing company, valuable information stored in its computer program is probably the majority of precious assets of the business that must definitely be protected. Access control is integrating with DB and information systems, in fact; it is a daily phenomenon. A lock on an automobile door is a form of access control essentially. A PIN on an ATM system at a bank is another method of access handle. The possession of entry control is of primary importance when persons look for to secure essential, confidential, or sensitive info and equipment. It is crucial that you appreciate that data should be protected not only from

exterior threats, but also from insider threats furthermore . Thus, trust but verify before providing DB access. Whether it is malicious or not, increased DB access can enhance the potential of insider threat but before providing DB entry verify. Whether it's malicious or not really, increased DB entry can enhance the possibility of "insider threats". A business is best offered by trusting those parties with DB entry while verifying through permissions, their access handle and defined roles and also monitoring instantly that their behavior drops within the authorized activity .

[VII] INTEGRATING INTRUSION DETECTION SYSTEMS FOR SECURING DB

Conducting normal audits will make sure that protection policies are on the right way and will help identify irregularities or possible breaches before it's too past due. Utilizing security auditing equipment will help in monitoring and documenting what is occurring within the DB and also it also offers alerts when suspicious or irregular activity occurs. Therefore MLC-DBS framework makes use of some notifications which alerts the authorized users of the DBs in the event of any unauthorized access activity being performed by an unauthorized user with a view to getting an entry into the DB and also if someone succeeds to obtain an entry into DB, the contents are not easily finding off because they are secured by any type or kind of encryption mechanism . Figure 1 shows implementation of this integration in the MLC-DBS framework.

[VIII] NOTIFICATION SYSTEM

Alongside securing the contents, access security is very important also. The DB is really a prime focus of attack by an eavesdropper with a view to steal the trick information stored in the DB. Therefore, the usage of the DB must be restricted so the intruder will not get entry into the DB. In order to avoid this, a notification mechanism could be applied which informs the authorized user concerning the unauthorized access occurring to the DB by sending a proper notification, to a tool like cellular phone, in order that such undesired incidents of unauthorized access attempts to the DBs could be restricted . Figure 1 shows implementation of notification system in the MLC-DBS framework.

[IX] MLC-DBS DIAGRAM

MLC-DBS framework protects DB against external attackers by using I&A, access control, notification system, and encryption layer. And it protects DB from an insider attacker by using audit, IDS, and digital signature. DB backup is utilized whenever damage occurs to DB.

The general diagram of the proposed MLC-DBS system is shown in Figure 2. The operation of MLC-DBS starts with I&A. At this stage, user identity is determined, and, his authorization level is defined. The proposed MLC-DBS functions could be defined as following the ability to create a DB, special tables, encrypt data and store them in the DB, decrypt and manipulate DB, create DB-backup and manage the digital signature of the DB contents for integrity checks.

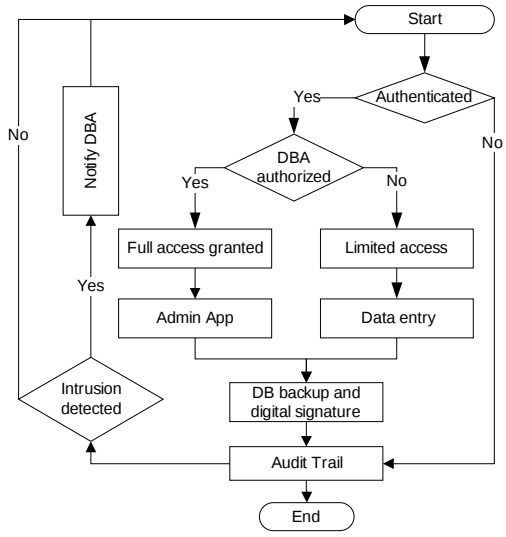

Fig: 2. MLC-DBS framework dataflow

[X] CONCLUSION AND FUTURE WORKS

MLC-DBS is an application to protect sensitive data. In spite of DB vulnerabilities, peoples still have no choice to store their own data in DB systems, so the need to secure DB systems becomes an important issue. Different approaches adopted to secure DB. MLC-DBS system may be favored under specific circumstances. There are many techniques and mechanisms of security, which differs from multi sides, reliability, requirement, cost, speed, policy… etc, which means, a technique may be the best for some place, whereas the same technique is totally insufficient for another place. MLC-DBS is the flexible solution, systems that protected by MLC-DBS are more secure than others, because, if one or some of the checkpoints are breakdown, there are other that remain the system in secure. The disadvantage of MLC-DBS is the complexity, which leads to make application not user friendly and costly and time consuming in design and maintenance phase. So a balance between security and simplicity (or transparency) is required since both are required. For next works we will present the detail diagrams and implementation steps of each layer, as well as DB's creation and main data manipulation tasks.

BIBLIOGRAPHY

[1] A. Kaur, “Securing Database using Public Key Infrastructure–A Proposed DB PKI Architecture,” *erpublications.com*, vol. 2, no. 5, pp. 44–47, 2013.

[2] A. Rezk and H. A. Ali, “Database Security Protection based on a New Mechanism,” vol. 49, no. 19, pp. 31–38, 2012.

[3] S. Asole and M. Mundada, “A Survey on Securing Databases From Unauthorized Users,” *Int. J. Sci. Technol. Res.*, vol. 2, no. 4, pp. 2–4, 2013.

[4] G. M. J, “Database Security : Best Practices for Securing The Database Of A Small Businesses,” vol. 2, no. 7, pp. 1–4, 2013.

[5] E. Site, R. Cuts, and S. In, “Security Engineering: A Guide to Building Dependable Distributed Systems,” 2ed Editio., 2008, pp. 239–274.

[6] A. Dwyer, M. Thuraisingham, D. Jelatis, and M.-D. S. Requirements, “Multi-level Security in Database Management,” vol. 6, 1987.

[7] N. Qader and L. Goerge, “Design and Implement a Secure Database Using Multi Level Security,” University of Sulaimani, 2007.

[8] P. B. Rane, “Application-Level and Database Security for E- Commerce Application,” vol. 41, no. 18, pp. 1–5, 2012.

[9] R. Tiwari, “A Novel approach for Hybrid

Database," *Int. J. Comput. Eng. Appl.*, vol. 1, no. 1, pp. 1–11, 2013.

[10] S. Scherzinger, M. Klettke, and U. Störl, "Managing Schema Evolution in NoSQL Data Stores," *arXiv Prepr. arXiv1308.0514*, 2013.

[11] S. A. Hossain, "NoSQL Database: New Era of Databases for Big data Analytics-Classification, Characteristics and Comparison," *Int. J. Database Theory Appl.*, vol. 6, no. 4, pp. 1–14, 2013.

[12] B. Lakshmi, "Data Confidentiality and Loss Prevention using Virtual Private Database.," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 03, pp. 143–149, 2013.

[13] V. Reddy and R. Krishnaiah, "ADVANCED CRYPTOGRAPHIC ALGORITHM FOR IMPROVED DATA SECURITY," Int. J. Comput. Eng. Appl., vol. III, no. III, 2013.