A RELIABLE DATABASE FRAMEWORK

Immanuel Gem Issac.A.J*, Vijesh Joe. C*, Balamurugan.C*
*Assistant Professor, Department of Computer Science and Engineering,
VV College of Engineering, Tisayanvilai
immanuelgem@vvcoe.org, vijeshjoe@vvcoe.org, balamurugan@vvcoe.org

ABSTRACT

A thing that can be compared with a valuable resources is data. We get data everywhere from various fields such as banks, government Sectors, Indian security forces etc. Most of these data's are stored in the database for analysis and future use. These valuable data's has to be stored and protected from mischievous behaviours from internal and external users. Speaking of protection the database need to be secured so that it can be used only by the authorized person at the right time of need. Even though there are multiple database protection mechanism in this paper we have discussed a model which is so Secure DBMS model. The prime goal of secure database management system(s-DBMS) is to provide information protection. While developing certain systems the economic consideration, trade-offs, performance should be taken care of. One who develops certain system should be careful not to be too secure. If developed too secure it will take too much of time in retrieval process or confusions while retrieving it back. Considering all these factors a S-DBMS model is introduced.

Keywords: Database, Security, Secure Database, Information Protection

I. LITERATURE SURVEY

While designing the database security is a vital parameter that has to be considered. For to check the system security level there are parameters that is taken into account which are availability, Trust ability and Integrity. In Addition to it there to give a complete database security authorization, auditability, and access control are taken in to account. In this it's also mentioned that the one who designs the database should have the knowledge on SQL operations.

Aziah Asmawi [2] in his paper defines threat in the database which can be addressed by the taking precautionary measures. Some measures discussed in this paper for the database security is by setting up policies. Also it's quoted that some safety mechanism are also to be added in order to protect the system database from auspicious and malicious attacks. By tuned safety mechanisms the database can also be secured from the intruders too. In addition to that it's been also discussed about SQL injection and protection strategies.

As per the author [3] marco Vieira and Henrique madeira changing the defects in the internal security can protect the database properly. This mechanism when configured rightly removes the hidden flaws.

According to conolloy [1] the database can be protected by adding importance to the controls that defends the system against the threats. The control should be taken on both system and non-system based .its discussed that if the design is so it can protect the other parts of the organizations along with the database.

As per this paper [4] security can be strengthened by considering protection on layer level. Multilevel layer protection for the computer system connected with database can be said as protected computer databases. By this analogy user level protection can be set in order to reduce the risk of attacks and threats.

II. DATABASE SECURITY

“Information security is the immune system in the body of business” by Kevin Pietersma, Information Security Architect, University of Toronto. As information technology become more reliable it increases the risk of vulnerable and inevitable breaches[5]. The breaches include unauthorized disclosures, alteration or theft of an organizations information and ultimately leading to privacy, legal and safety impacts. There are various laws to govern the use and disclosure of private information.

2.1. Defining database security

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. There are three functional areas to enforce data protection.

1. Security policies (what the systems expected to do)

2. Security mechanisms (how system achieves its goal)

3. Security system assurance (security requirements)

2.2. Maintaining secrecy

An effective system is one which keeps the data in secrecy during transactions. The commonly used system is BLP or Bell-LaPadula[7]. The BLP model was developed for the US government in the early ’70s. The BLP model proved that it is a secure DBMS for many years.

2.3. The BLP model

The model has two main abstract elements objects (passive entity) and subjects (active process). The object has four classification: unclassified, confidential, secret, top secret. Subject is the active process which requests access based on its clearance. An action class is said to be a combination of object and subject. The action classes are sorted and a lattice is formed. It determines whether to allow access or not. This is called flow control. The BLP model has two properties that describe the secure flow of information: The simple security property and the star (*) property. The simple security property can be described as the “no read up” rule. A subject must not be able to obtain information form clearance level higher than its current level.

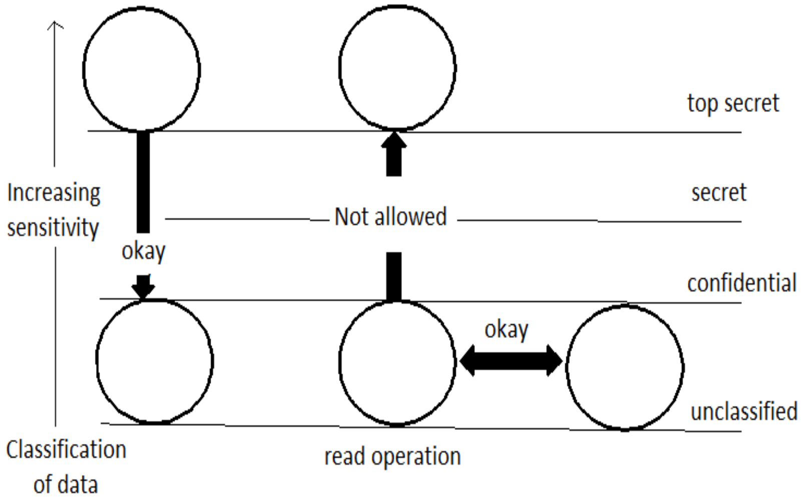

fig1: simple security property

The second BLP property is the star (*) property. The * property is known as the “no write down” property [7]. The *-property maintains information secrecy by not allowing a higher classified object to be lowered or declassified.

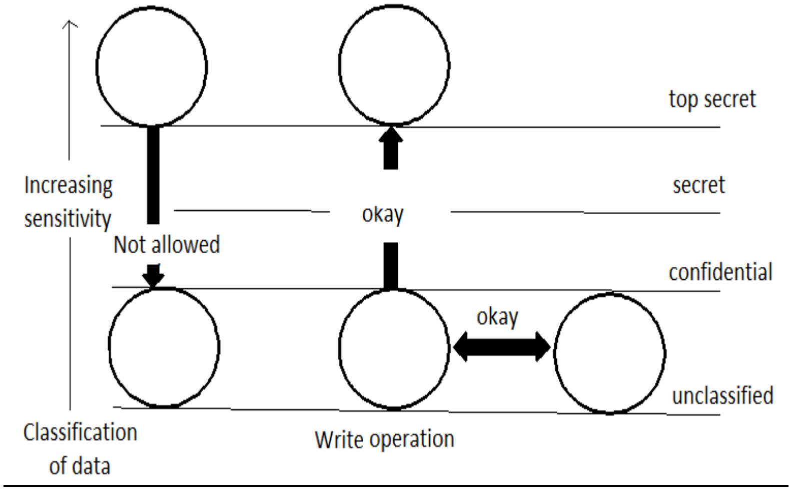

fig2: blp (*) property

III SECURITY POLICIES

There are two types of security policies: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). The typical DAC security policy implementation in an S-DBMS is based on granting and revoking privileges. The privileges are of different levels. Access is granted or denied based on the identification of user[11][12]. Unlike DAC, MAC requires users to follow certain rules in order to access the information. It works in combination of objects and subjects. The MAC policy requires the objects to be classified and subjects to be cleared. The attributes of subject and object can only be modified by the authorized administrator. MAC only allows users to modify information based on their clearance. DAC and MAC can coexist in a single S-DBMS.

IV. SECURITY MECHANISMS

Security mechanisms implements the set of rules or policies of an S-DBMS. It can be in the form of software, hardware or administrative procedures. There are three phases 1) preventing mechanisms 2) detecting mechanisms 3) recovery mechanisms. Each of the mechanisms has its own kind of threat and possible counter measures[6]. A preventive mechanisms prevents a cyber-attack by posing as a barrier or firewall or any other type of blocking methods. A detecting mechanism detects a system breach and reports the administrator by setting off an alarm or by using an audit trail to monitor unusual system activities. A recovery mechanism restores the system, to its state before a successful breach by using backup tapes or redundant hardware [9][15].

4.1. Security system assurance

System assurance is used to overlook all the security mechanisms by maintaining proper consistency and integrity[13]. The goal is to provide system recovery under operating conditions.

4.2. Problematic Issues

Three major security issues are confidentiality, integrity, availability. Confidentiality refers to the access of information to the authorized users. Any unauthorized access must be prevented. There are three database integrities physical database integrity, logical database integrity, data element integrity. Physical database integrity protection involves power shutdown and fire accidents. Logical integrity protection refers to modification of data by the authorized users and preventing others. Data element integrity protection refers to data assurance and accuracy [8].

The final issue is that to maintain data in the user authorized domain. If protection is not effective enough, the attacker may target certain weak spots in the system and exploit certain piece of information or totally block the access of the user.

V. SECURITY THREATS

An action which causes breach or violation of any kind is considered a security threat. There are two types of threats: accidental and intentional threats. Accidental threats are the ones which occur hardware failure, natural disaster, etc[10]. They may even be caused by software bugs. An intentional threat is one where an attacker or so called hacker finds a loophole or blind spot in the database and attacks it and steal information without authorization.

5.1. Control measures

Control measures are implemented to reduce accidental threats and intentional threats. The basic two types are operational measures and technical measures. Operational measures are implemented in our daily life in protection of systems and applications[14]. The protection involves physical access control, intrusion detection, and fire, water, moisture, heat and electrical protection. Technical measures are which involves hardware and software implementation to automate protection of information of systems and applications. Some technical controls might be user identification and passwords or tokens, audit trails, cryptography or software products to scan, detect and remove computer viruses.

VI. CONCLUSION

A database is said to be secure database system if it satisfies certain parameters such as user friendly, fast processing, and transaction secrecy. Adaptability is the other main feature a secure database should have to support the changing needs at state. On taking all these parameters in to count the database should not be violated on security aspects. Also the whole environment should be considered for the aspect database security .

REFERENCES

1] Connolly, M. & Begg, C. (2005). Database systems. A practical approach to design, implementation and management. (4th ed.). Harlow, Essex, England: Addison-Wesley (Pearson Education Limited).

[2] Aziah Asmawi , "System Architecture for SQL Injection and Insider Misuse Detection System for DBMS", my -1-4244-2328 6/08/$25.00 © 2008 IEEE

[3] Marco Vieira, Henrique Madeira, "Detection of Malicious Transactions in DBMS", 11th Pacific Rim International Symposium on Dependable Computing

[4] DOD Computer Security Center: Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD- 001-83, August 15, 1983.

[5] Dwyer, D. Jelatis &and M. Thuraising :Multi-level Security in Database Management Systems, Computers and Security, vol 6, no. 3, pp. 252-260, 10.1016/0167-4048(87)90106-4

[6]Faragallah, M. El-Rabaie , El-Samie, I. Sallam and S. El-Sayed:"Multilevel Security for Relational Database".ISBN: 9781482205398 - CAT# K21447

[7] Abram, M. and Olson, I. (1990). "Computer Access Policy Choices", Computer and Security. Pp. 699-714.

[8] Abrams, M, Jajodia, S, and Podell, H, eds, Information security: An integrated collection of Essays, IEEE Computer Society Press, 1995

[9] Adams, Anne and Sasse, Martina Angela, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, 42(12):4046,December1999http://www.acm.org/pubs/contents/journals/cacm/1999-42/#12

[10] Atzeni,P. and Antnellis, D. (1993). Relational Database Theory. Benjamin/Cummings

[11] Audit, NCSC Technical Report – 005

[12] Bertino, Elisa, Jajodia, Sushil and Samarati, Pierangela, DatabaseSecurity: Research and practice, Journal of Information System,May 1995

[13] Bhaskar, K, Computer Security: Threats and Countermeasures,published by NCC Blackwell, 1993

[14] Castano, S, Fugini, M.G, Martella, G,and Samari, P, Database Security, Addison-Wesley, 1994

[15] Csilla, F. (2000). Discrete Access Control. O'Reilly Associates, Inc.