

A Comprehensive Summarization about Cyber Security and Database.

¹Shreya Suryawanshi,
Sinhagad Institute of Technology Lonavala.

Date of Submission: 09-01-2023

Date of Acceptance: 19-01-2023

ABSTRACT-

In today's technological world as the new technologies are developing the cyber-attacks are also increasing. The big organizations are facing the big issues about securing their database. The sensitive data stored in database is at high risk which may lead to big loss to that organization. So, the awareness about the various cyber threats is need to develop among the people. This review gives the information about the different cyber-attacks and the ways to avoid them.

Keywords- Cybersecurity, Database, Cyber-attacks.

I. INTRODUCTION-

Considering the importance of data, it is essential to secure that data. Protecting the sensitive or the confidential data stored under a warehouse is termed as the database security. Database security is a vital aspect that any organization should take special care in order to run its activities efficiently [1].

There are different kinds of threats may be seen in database such as intentional or accidental loss of data, distortion as well as misuse of data. These threats may lead to the loss of confidential data so as a prevention measures organizations paying more attention on monitoring their database so that they can avoid such loss of data [1].

The data that is available on the Web can be protected by providing protection from DoS attacks [2].

These cyberattacks are highly sophisticated, targeting governments and large-scale organizations. To overcome these issues

database need strong antivirus to detect the malicious activity happening in database [3].

Most database store sensitive data for users which can be sensitive for hacking and misuse. Therefore, organizations have greater controls and checks on their database to maintain the security of the information and make sure that their system are monitored closely to avoid inappropriate activities in database [4].

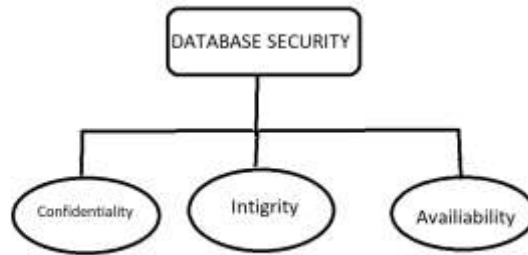
Some of Latin American countries follows laws that guarantee data protection guidelines that are stored in each of the public organizations. The associate editor coordinating the review of this article and approving it for publication was KaiguiBian[5].

The cyber attacker enters in a processor and make changes to the number of votes of one or more candidates, these kind of problem can be very sensitive and emotional to the voters as well as for the candidates. The United States blames Russia for hacking the emails of Democratic party and al the presidential candidate [6].

As the database security is a crucial problem for big or public organizations they are now giving more attention to securing their database so that the hackers will not misuse their confidential data from the database [6].

Due to the upgradation in the technology used in database there are lot of good things are happening but also the several loopholes are formed for attackers or hackers and due to this the database can be often attacked. Thus in result the improvement in the hackers technique cannot be prevented by traditional methods. Now days machine learning has more acceptance rate rather than the traditional methods [7].

Confidentiality, Integrity, Availability these are the main three factors of database security [6].



Previous work about database security-

There is lot of work done in order to provide security to database. According to the previous work various techniques are given for database security such as

Authorization :- Which is related to grating rights for accessing any particular data.

Audit Trail :- This technique is used to check the history operations.

Access control :- This technique will give right to access the data after verifying the accessing request which help to avoid unauthorized access[4].

On the basis of various security parameters empirical analysis is given using encryption method[8].

Security Parameters	Frequency	Percentage	Criticality
Confidentiality	5	100 %	Very High
Integrity	2	40 %	Moderate
Access control	2	40%	Moderate
Efficiency	2	40%	Moderate
Privacy	3	60 %	High

Fig 1. Empirical Analysis of security parameters achieved using Encryption methods [8].

Data encryption is a basic technique used to secure any kind of data or information.[9]



Fig 2. Data Encryption [9].

MalNet is largest and publicly available cybersecurity image database. There are some properties of MalNet like Scale, Hierarchy, Diversity & Imbalance, Cybersecurity Applications[10].

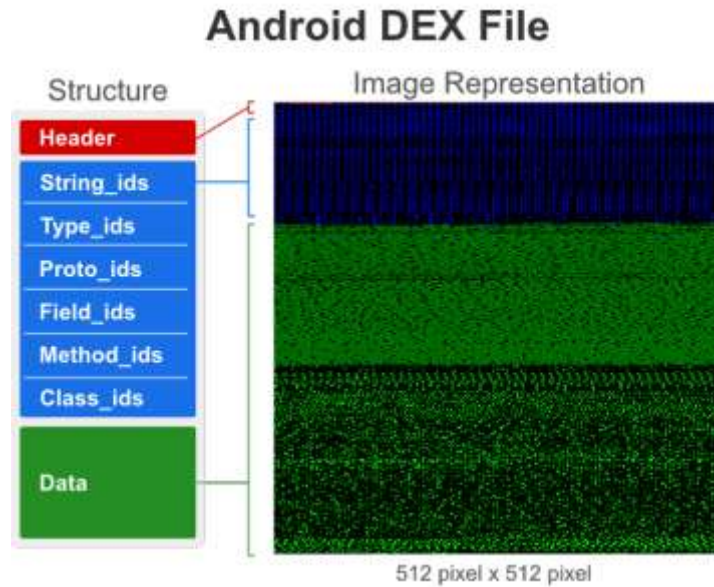


Fig 3. Left-side: structure of an Android DEX file. Right side: image representation of DEX file [10].

Malware Images with Varying "Texture"

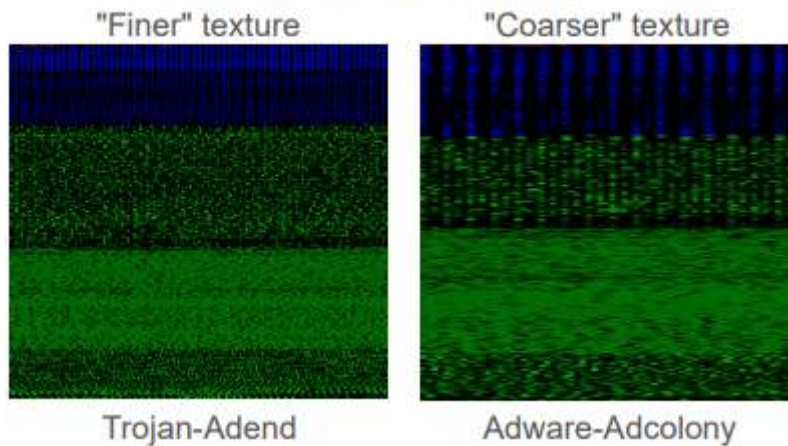


Fig 4. Images of two malware types with different "texture".

Left: the Trojan image is more "fine-grained". Right: the Adware image is more "coarse"[10].

There are some applications of Malnet
 Application 1: Benchmarking Techniques
 Application 2: Malware Detection

Application 3: Malware Classification[10]
 GLOBAL ATTACK REPORT[11]:-

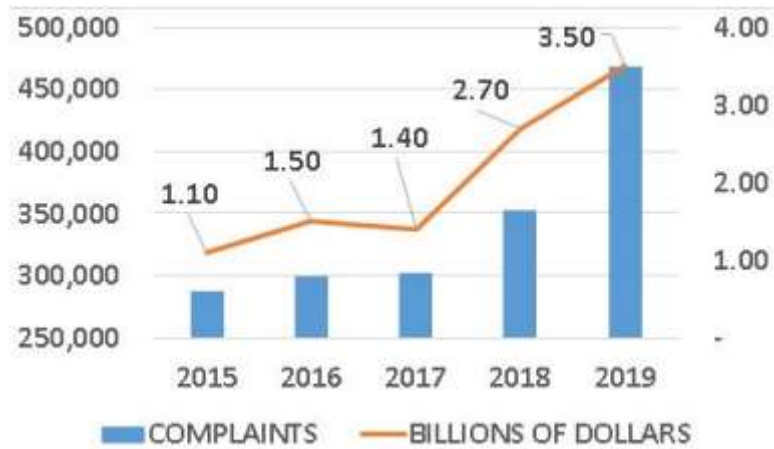


Fig 5. Reports vs billions of dollars globally [11].

These are some results to avoid cyber attacks:-
 Evaluation prototype of a database security model
 Blockchain security management architecture
 prototype for a database
 Algorithm prototype of security for databases
 Logical structure of the management system on
 Blockchain
 Prototype to mitigate Cyber Attacks[11].

To prevent the cyber attacks we need to achieve
 security measures at various levels[12]:-
 Database systems.

Operative System.
 Network.
 Physical.
 Human.

There are different levels in accessing the
 database[12]-
 Discretionary Access Control
 Mandatory Access Control
 Closed

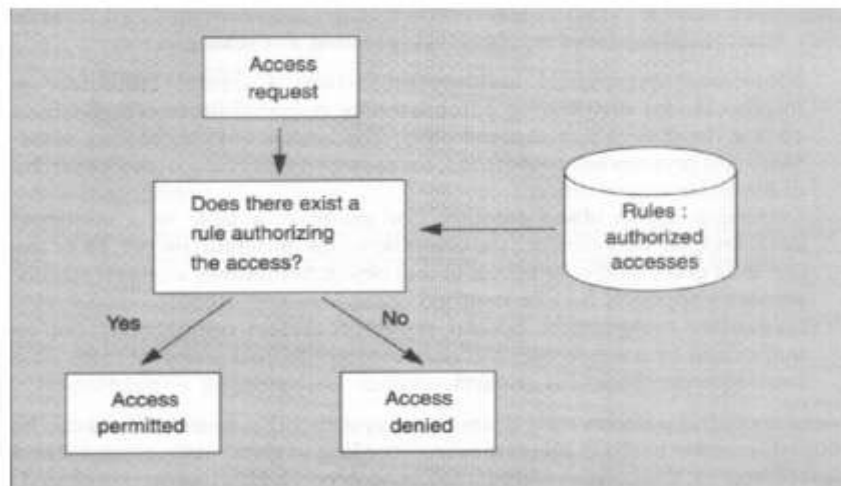


Fig 6. Closed: Only authorized accesses are explicitly allowed[12].

Open

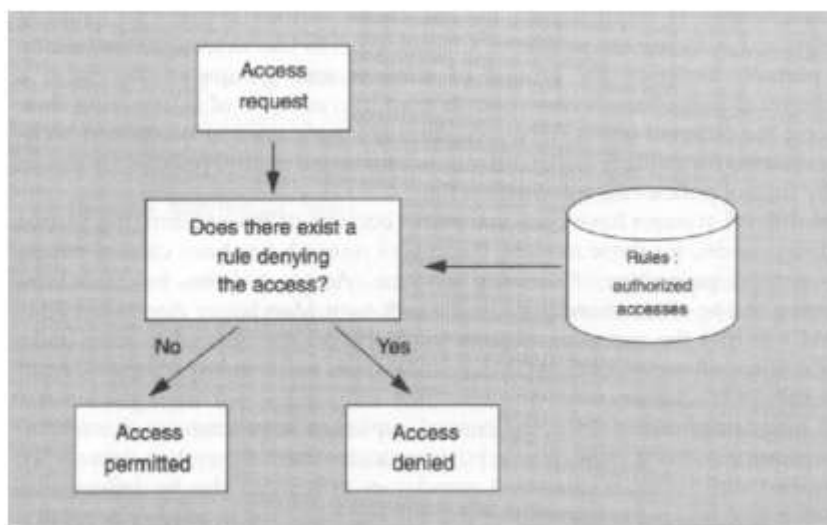


Fig 7.Open: the access not forbidden are allow [12].

II. CONCLUSION-

This paper focuses on the various types of cyber attacks and different ways to avoid them. The previous research about database security gives the awareness about how can the big organizations save their sensitive data from cyber attacks. In this paper we discussed several techniques in order to save the data from attackers also we saw the basic method that is data encryption which is widely used in today's technological world to create the security about the sensitive or critical data.. Currently, no large-scale public database exists to assist researchers and practitioners in this important topic. According to survey 84% of companies says that the database security is really very important topic nowadays. Also 48% of authorized users are the attackers they misuse their privileges. As the world's business leading to online and cloud data storage and management, **demand for cybersecurity is at an all-time high**. As a result, there is a greater demand for cybersecurity skilled in Artificial Intelligence and Data Science. So in conclusion we can say the cybersecurity is the leading and hot topic in technology world.

Acknowledgement-

The authors are thankful to Dr.M.S. Gaikwad, Principal Sinhagad Institute of Technology Lonavala for his continuous motivation, support and providing the necessary infrastructure to carry out this work.

REFERENCES-

[1]. Snehrathore, Anupam Sharma "Database Security- Attacks, Threats and Challenges" International Journal of

Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICCCS - 2017 Conference Proceedings

- [2]. E. Bertino, D. Leggieri, and E. Terzi "Securing DBMS: Characterizing and Detecting Query Flood," Proc. Ninth Information Security Conf. (ISC '04), Sept. 2004.
- [3]. Scott Freitas, Andrew Wicker, Duen Horng Chau, and Joshua Neil. D2m: Dynamic defense and modeling of adversarial movement in networks. In Proceedings of the 2020 SIAM International Conference on Data Mining, pages 541–549. SIAM, 2020. 1
- [4]. Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili "Security in Database System" .Global Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 17 Version 1.0 Year 2012 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.
- [5]. S. M. T. Toapanta, J. D. L. Cobeña, and L. E. M. Gallegos, "Analysis of cyberattacks in public organizations in latinamerica," Adv. Sci., Technol. Eng. Syst. J., vol. 5, no. 2, pp. 116–125, 2020, doi: 10.25046/aj050215.
- [6]. Preeti Sharma "Database Security: Attacks and Techniques" .International Journal of Scientific & Engineering Research,

- Volume 7, Issue 12, December-2016 313
ISSN 2229-5518.
- [7]. Meng, J. (2018) Security Threats and Countermeasures of Computer Network Database. PC Fan,23, 37-37.
- [8]. Iqra Basharat, Pakistan Farooque Azam, Islamabad, Pakistan Abdul Wahab Muzaffar “Database Security and Encryption: A Survey Study” International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.
- [9]. Shivnandan Singh, Rakesh Kumar Rai” A Review Report on Security Threats on Database” Shivnandan Singh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3215 – 3219.
- [10]. Scott Freitas,Rahul Duggal, DuenHorng Chau “MalNet: A Large-Scale Cybersecurity Image Database of Malicious Software’ Georgia Institute of Technology {safreita, rahulduggal, polo}@gatech.edu.
- [11]. SEGUNDO MOISÉS TOAPANTA 1 , OMAR ALEXANDER ESCALANTE QUIMIS 1 , LUIS ENRIQUE MAFLA GALLEGOS 2 , AND MA ROCÍO MACIEL ARELLANO 3” Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks” Received July 17, 2020, accepted August 31, 2020, date of publication September 10, 2020, date of current version September 25, 2020. Digital Object Identifier 10.1109/ACCESS.2020.3022746.
- [12]. Domínguez Chávez Jorge” Basic Principles of Database Security”, Universidad Politécnica Territorial del estado Aragua.