IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 25-28

A Review on Database security threats

Mrs. Rama Sanjay Bansode[1], Maitreya Tambade[2], Dr. Anup Girdhar[3]
[1]*(PhD Research Scholars in TMV, (Faculty in Modern College of Engineering, Pune),*
[2]*(Student Modern College of Engg., Pune)*
[3]*(PhD Guide Tilak Maharashtra University, Pune)*

Abstract: *Data security is an important issue and a growing concern that affects all sectors in this modern era. Lack of data security can lead to confidential information being accessed by unauthorized persons & the integrity of information gets compromised. In light of these, the present study addresses data security. Findings reveal that data security is an important area, worthy of attention. As such, data security threats & data protection strategies are studied in this paper.*

Keywords: *Database , Database systems, RAID, Data Security, Data Protection, Media Failure, Storage System Failure, Data Corruption, Data Center Failure, Digital Privacy, Cyber Crimes, Net Morality, Cyberspace issues, Domain issues, Virus, Hacking*

I. Introduction

Database & Database systems are essential components of everyday life in Modern Society in this digital era. In our Daily life we encounter with several activities which involves some interaction with database & Data Systems.

Due to huge use of Smart Phones, Computers & various electronic devices the huge amount of data regarding the user is collected. This huge amount of data is also termed as Big Data it is a collection of data sets which is very large in size as well as complex i.e. the size of the data varies between Petabyte and Exabyte. Big data is one of the most talked topics in IT Industry playing an important role in our day to day life.[1][2]

Various Data Management tools are used in order to manage this big data. It is also important to maintain the privacy & Security of the data. Due to advancement in security companies are consulting and gaining more and more data about their clients & hence the protecting data & maintaining its security is important in this Digital Age.

II. Research Methodology

This research used a literature review approach to collect and analyze existing findings of research with regards to information security in the digital age. This approach is suitable to provide a summary of literature of identified problem and the resultant objectives of the study.

III. Purpose ofData Protection

The process of safeguarding the important information & data from corruption, compromise or loss is termed as Data Protection. The importance of data protection increases as the amount of data created and stored continues to grow at very high rates. All most all Organizations frequently move their backup data to public clouds or clouds maintained by backup vendors. These backups are replaced on - site disk and tape libraries, or they can serve as additional protected copies of data.

Traditionally Data Backup has been the key to an effective data protection strategy. Data is periodically copied, to a tape drive or tape library or hard disk drives i.e. the primary data storage. That's how when is damaged we can recover & restore lost or damaged data. However, backups are no longer a stand-alone function. Instead, they're being combined with other data protection functions to save storage space as well as maintain the lower costs.

Previously backup and archiving, were been treated as two separate functions. The purpose of data backup is to restore data after a failure, while an archive provided a searchable copy of data. However, that led to redundant data sets. In today's Market, there are products that back up, archive and index data in a single pass. This approach saves organizations time and cuts down on the amount of data for long-term storage.

IV. Data Failure Threats

In today's date the data protection for primary storage involves using a built-in system that supplements or replaces backups and protects against the following potential problems:

- Media Failure

- Data Corruption
- Storage System Failure
- Full on Data-Center Failure

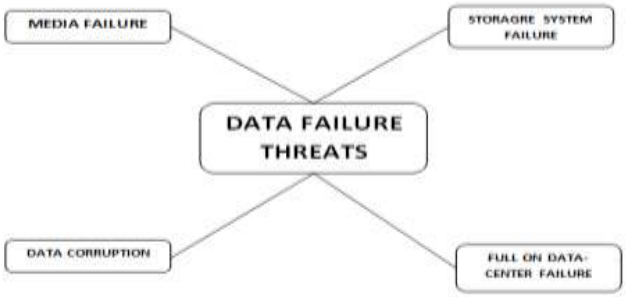

Fig.1 Data Failure Threats

Media Failure

The goal here is to make data available even if a storage device is failed. Synchronous mirroring is one approach in which the data is written to a local disk and a remote site at same time. The write is not considered complete until a confirmation is sent from the remote site, ensuring that the two sites should be always identical. Mirroring requires 100% capacity overhead.[4]

Another approach to recover the data during media failure is RAID (redundant array of independent disks) protection is an alternative that requires less overhead capacity. With RAID, physical drives are combined into a logical unit that's presented as a single hard drive to the operating system.Which enables to store same data in different places on multiple hard drives. As a result the Input /Output operations areoverlapped in a balanced way, by improving performance and increasing protection. [5]

Data Corruption

When accidentally data gets corrupted or deleted, snapshots can be used to set things right. Most storage systems today can track the snapshots without any significant effect on performance.

Storage systems using snapshots can work with some Key applications like Oracle and Microsoft SQL Server, to capture a clean copy of data. This approach enables to store frequent snapshots for long period of time.

Storage System Failure

To protect the data against multiple drive failures or some other major event, data centers rely on replication technologies which were built on top of snapshots.

With snapshot replication, the only blocks of data that is changed are copied from the primary storage system to an off-site secondary storage system. Snapshot replication is also used to replicate the data to on-site secondary storage that are available for recovery if the primary storage system fails.

Full-on data center Failure

To protect the data against the failure of whole data center requires a full recovery plan. As with the other failure scenarios, there are multiple options to recover the data in such case. **Snapshotreplication**, where data is replicated to a secondary site, is one of option but the cost of running a secondary site can be expensive. Cloud services are another option. Cloud backup & Replication products and services are used to store the most recent copies of the data that is most likely to be needed in the major disaster. This results in a rapid recovery in the event of a data center failure.

V. Data Security

The protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites are known as Data Security. Data security also protects data from corruption. It is very essential aspect of IT for organizations of every size and type. The term Data security is also known as information security (IS) or computer security.[3]

One of the important reasons to implement data protection strategies is fear of financial loss. Data is recognized as an important corporate asset that should be safeguarded. Loss of information may lead to direct financial losses, such as lost sales, fines, or funds. [1][6]

Types of Security Threats:

- **Internet Based Scams & Crimes**
- **Cyber Crime through Virus & Hacking**
- **Cyberspace(Domain) Issues**
- **Net Morality**
- **Internet Control/ Security Management**

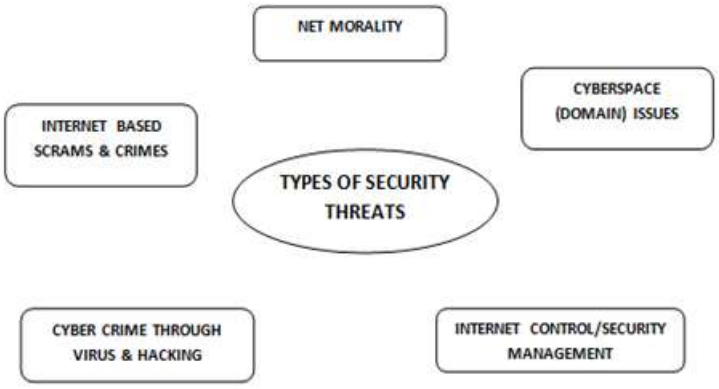

Fig.2 Types of Security Threats

Internet Based Scams & Crimes

A scam is tricking a person to steal money & important data by using internet there have been observed criminal behaviors possibly motivated by fun exploiting SNS (Social Networking Sites). A major example is theft of social media ID, such as Twitter ID, of a celebrity or actual company.

The best defense against this type of scams on the Internet is, just like in the real physical world. Here just People should be cautious about their information while using the Internet. [6]

Cyber Crime through Virus & Hacking

Stealing of information stored on PC or other devices like mobile & tablets using virus or hacking a server or bypassing authentication is typical cyber-attack techniques. These attacks are likely motivated by financial gains and the scale of the damage is getting bigger every year. The use of sophisticated techniques of Computer Science technologies or tools available on internet in order to steal the information with Money is done by attackers.

It is important to implement the appropriate security measures to PCs, servers & every device which is connected to internet and use them safely. [6]

Cyberspace (Domain) Issues

Nowadays the cyber-attacks have become a matter of international politics because cyberspace has been recognized as a domain that can be used to achieve foreign affairs and national security, or military campaigns. Thus, it must be considered as a different issue from traditional information security.

Cyber-attacks are already a main theme in international politics which were addressed in the U.S.-China summit in June 2013. International politics seek a way cyberspace is utilized safely by all the nations like territorial lands and territorial waters. [6]

Net Morality

Net morality is a serious issue not only at young student generation but also for adult generation since all are using the Internet today. With the prevalence of SNS, we now have an environment where people can easily share their private information or things happened at work with others to receive attention. However, to live in a society, we must show a certain level of morality. [6]

Internet Control/ Security Management

Corporate accounting scandals in early 2000's led a discussion about internal control and compliance in Japan. However, establishing an information security management system has been a popular move among businesses and organizations since Mid-2000's. The basics of internal control and compliance are to protect an organization's data information assets (i.e. data and systems) from intentional or accidental leak, falsification, deletion and/or disruption by establishing data security controls. [6]

VI. Conclusion

In todays, Digital Era the importance of information & Data is key in all sectors of the economy and at all levels of human endeavor. Data is relevant to organizational success, individual achievement, effective managerial decisions, and national development. & hence it is very important to protect the data & maintain its security. The utmost attention should be given for data handling, data protection and data security to protect the economy and social gains.

References

[1]. Paper on: Information Security in the Digital Age: The Case of Developing Countries. *Chinese* Librarianship: an International Electronic Journal, 42.
[2]. 2014 Edition 10 Major Security Threats, IT SECURITY CENTER (ISEC) ,INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
[3]. Fundamentals of Database Systems Author: RamezElmsri
[4]. Data Protection : https://searchdatabackup.techtarget.com/definition/data-protection
[5]. RAID : https://searchstorage.techtarget.com/definition/RAID
[6]. Data Security : https://searchsecurity.techtarget.com/feature/Overwhelmed-by-security-data-Science-to-the-rescue