Database Security Threats and How to Mitigate Them

Ms. Sushmita Chakraborty
Research Scholar
Shri Venkateshwara University
Gajraula Amrohi U.P.
Mobile No : 8084854045
Email-id: sushmita.mca@patnawomenscollege.in

TRACK: 2

Database Security Threats and How to Mitigate Them

Ms. Sushmita Chakraborty
Research Scholar
Shri Venkateshwara University
Gajraula Amrohi, U.P.
Email-id: sushmita.mca@patnawomenscollege.in

Abstract

The most important resources for an individual as wells as for any organizations is data. Taking into account it is important to secure the data. Applications are often the source of most database security threats and much can be done within a database to promote effective security. As we know, the info has been one among the foremost most popular selections of the hackers. the explanation behind why the databases ar targeted thus ofttimes as they're the center of any organizations. It is observed that organizations are also not protecting these crucial assets well enough. They find it difficult how and what is needed to secure a database and who within the organization is responsible. Therefore, Data Base Management System approach is a challenging task and database security threats is one of the important aspects that organizations should take special care in order to mitigate them in order to run the activities of the organizations efficiently. A brand new report by ***Dark Reading*** *stated that there are varieties of key security failures that cybercriminals make the most of data breaches. The database developers, administrators, staff members of the organizations who create the environment necessary for attacks to gain access to data. There are many vital ways that are usually accustomed to steal knowledge directly from database files, from database backup files, by intercepting the database traffic and using unauthorized access. Database Security is not only the sole responsibility of a database administrator (DBAs). There are several components involved to secure the database. The security of an organization's data is the responsibility of the entire organization, from executive management to operations and IT, from network and security to compliance, legal, and risk personnel. The aim of this study is to review what are the various information Security threats, vulnerabilities and security challenge that require to be thought-about still as new technological tools a way to mitigate information security threats.*

Keywords: *DBMS (Database Management System), Database Security Threats, Mitigate, IT (Information Technology), DBA (Database Administrator)*

I. INTRODUCTION

Data forms one amongst the foremost necessary resources for a personal as well as for any organizations. Maintaining information and organizing them properly may be a vital task. Security is one of the foremost necessary and difficult tasks within the e-world that the whole world is facing in every aspects of life. Organizations will notice it tough however and what is required to secure a information and WHO inside the organization is responsible. It is necessary to protect the sensitive and confidential information underneath a store home which is referred to as the information security. Information has perpetually been one amongst the foremost most popular decisions for the attackers. A huge variety of industries unit ceaselessly becoming a victim of cyber crime. A company ought to take special care from information security purpose of read in order to run its system with efficiency. It's an effort in protecting any non-public information against threats like international or any kind of accidental loss or misuse. The threat is a kind of challenge in terms of the integrity of the information and access management. Information protection cares by varied gears of a DBMS. As per the researchers over a 3rd of assess databases area unit missing security updates or running previous version of the computer code. Such cases show that a lot of firms or organizations don’t have a reliable and consistent patch-management and info security system that is a reality worrying fact. The organizations that take this variation ought to contemplate that the applying should be in-built such how thus on store all the sensitive information in encrypted kind. Lastly when talking about the concurrency management method and also the recovery scheme takes care of the provision of accurate knowledge inspite of any package or failure of hardware and also the accesses made up of some synchronal application programs.

Strategic objectives for a good information Security are :

1. To minimize the attack surface

2. To Categorize databases and act suitably

3. To carry out intelligent and business-focused auditing and watching.

When talking about effective security, whether or not Information Technology or any sort of security. Two key ideas should be included:

1) Security may be a method

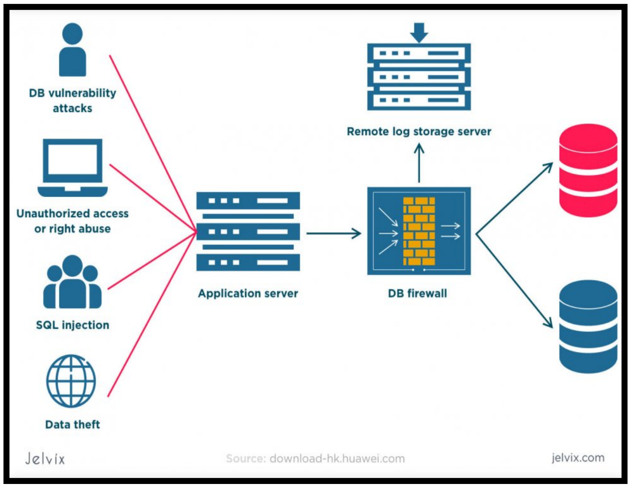
2) for defense comprehensive.

Securing the information may be a powerful task for varied reasons, however the foremost vital is that the assortment of area rather than an area of its own.

II. DATABASE SECURITY ATTACKS

Database Security means protection of that data which means external sources could never access the data. It means the information that is stored in the data warehouse or repository can never be accessed or read by any individuals or organizations without any authorization. Database security refers to the range of tools, controls and measures, which is designed to establish and preserve data bus which means confidentiality, integrity and availability.

Table : 1



Source: https://jelvix.com/blog/database-security

The main focus is on confidentiality because it is the element that is compromised in most of the data breaches. Database security must protect and deal with following: [11]

- The database management system(DBMS) [7]
- Any associated applications[7]
- The physical server and /or the virtual database server and the underlying hardware[7]
- The computing and /or network infrastructure used to access the database.[7]

Database security is a difficult and challenging endeavour that takes into account all the features of information security, Technologies and practices. The more the database is accessible the more vulnerable and it becomes a challenge to security threats; the more invulnerable the database is to threats, the more difficult it is to access and use.[12] The question arises how much harm a data breach inflicts on your enterprise depends on a number of factors:[9]

- Whether to compromised with intellectual property
- How it damage to brand reputation
- Business continuity (or lack thereof)
- To impose fines or penalties for non-compliance
- Costs of repairing breaches and notifying customers[7]

III. Most Significant Risks of 2015 and How to Mitigate Them

Databases are considered to be the most compromised property according to the **(2014 Verizon Data Breach Repor**t) [4]. The main reason why databases are targeted so often is quite simple. They are the core heart of any institution or enterprise, storing and maintaining the customer records and other confidential business data. The question arises why are databases so vulnerable to breaches? One of the reasons is that organizations are not protecting these crucial assets well securely. According to International Data Communication, less than 5% of the $27 billion spent on security products directly addressed data center security. [4]

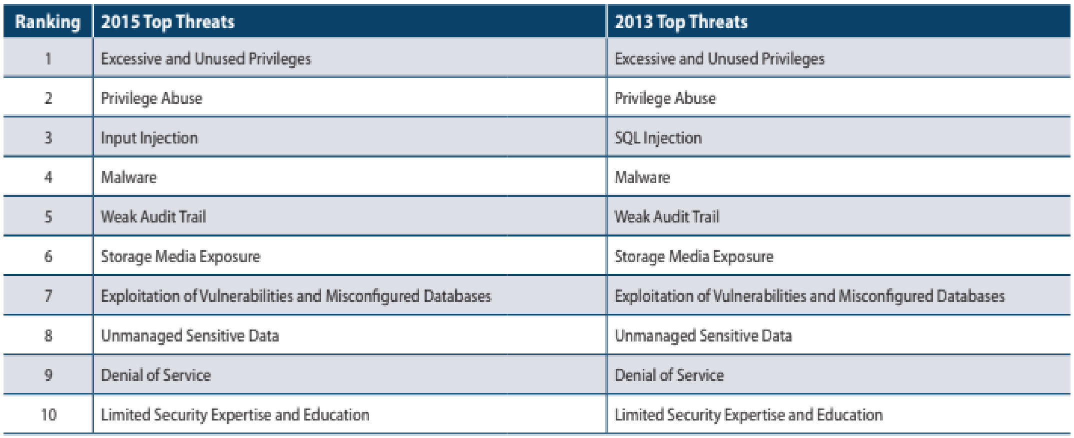
Whenever the hackers and malicious insiders gain access to these sensitive data, they can extract value, inflict damage, and can make an impact on business operations. But in case of financial loss or reputation damage, breaches can result in regulatory violations, fines, and legal fees. However, the good news is that the vast majority of incidents – more than 97% according to the Online Trust Alliance (OTA) in 2013– could have been prevented **[4]** by implementing simple steps and following best practices and internal controls. **[4]**

The top ten threats which is stated in the whitepaper **Imperva Application Defense Center** apply not only to traditional databases, but also to Big Data technologies. While Big Data's NoSQL technology is different from SQL, the same injection points – such as input fields – still exist for Big Data. **[4]**

Database Security Threats: 2013 vs. 2015

According to the white paper highlights the ten most critical database threats as identified by the **Imperva Application Defense Center.** The same threats can be seen in 2013 which continues to harm businesses. A prominent change is renaming the “SQL Injection” threat to “Input Injection” to reflect its significance to Big Data technology. [4]

Table : 2



Ranking	2015 Top Threats	2013 Top Threats
1	Excessive and Unused Privileges	Excessive and Unused Privileges
2	Privilege Abuse	Privilege Abuse
3	Input Injection	SQL Injection
4	Malware	Malware
5	Weak Audit Trail	Weak Audit Trail
6	Storage Media Exposure	Storage Media Exposure
7	Exploitation of Vulnerabilities and Misconfigured Databases	Exploitation of Vulnerabilities and Misconfigured Databases
8	Unmanaged Sensitive Data	Unmanaged Sensitive Data
9	Denial of Service	Denial of Service
10	Limited Security Expertise and Education	Limited Security Expertise and Education

Source : e763d022-6ee4-4215-9efd-1896b0d9c381_wp_topten_database_threats imperva.pdf [4]

Database Security Common Threats

Table : 3

- Excessive and Unused Privileges
- Privilege Abuse
- Input Injection (Formerly SQL Injection)
- Malware
- Weak Audit Trail
- Storage Media Exposure
- Exploitation of Vulnerable, Misconfigured Databases
- Unmanaged Sensitive Data
- Denial of Service
- Limited Security Expertise and Education

Excessive and Unused Privileges
Privilege Abuse
Limited Security Expertise and Education
Input Injection
Denial of Service
Database Security Threats
Malware
Unmanaged Sensitive Data
Weak Audit Trail
Exploitation of Vulnerable, Misconfigured Databases
Storage Media Exposure

Database Controls and Policies

Apart from implementing layered security controls across the entire network, database security requires to set up the correct controls and policies for accessing of the database. These include:

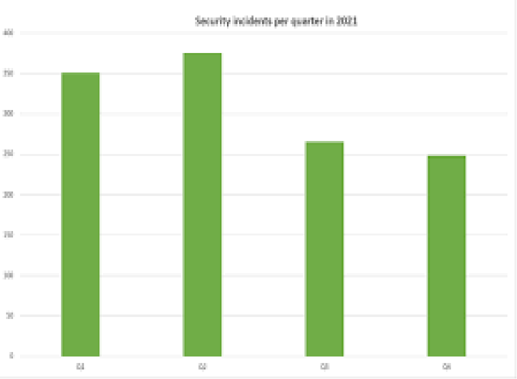
- **Administrative controls :** to govern installation, change, and configuration management for the database.[7][8]
- **Preventative controls:** to govern access, encryption, tokenization, and masking.[7][8]
- **Detective controls**: to monitor database activity monitoring and data loss prevention tools. These solutions make it possible to identify and alert on anomalous or suspicious activities.[7][8]

Database security policies have to be incorporated in order to support the overall business goals like protection of crucial material possession, cyber security and cloud security policies. It is very much important to make sure that the user have to take the responsibility for maintaining and auditing security controls among the organization which your policies complement those of your cloud supplier in shared responsibility agreements. Security controls, security awareness coaching, education schemes, and penetration testing and vulnerability assessment ways ought to all be established in support of your formal security policies.[7]

IV. DATA BREACHES AND CYBER ATTACKS IN 2021

5.1 billion breached records are found during data breaches and cyber attacks in the year 2021. According to IT Governance 1,243 security incidents in 2021[5] was discovered, which stated for 5,126,930,507 breached records. That shows an 11% increase in security incidents compared to 2020 (1,120).[5] According to the graph there was a significant decrease in the number of breached records over the same period (20.1 billion).[5]

Table : 4



source:https://geekflare.com/database-threats-and-prevention-tools/

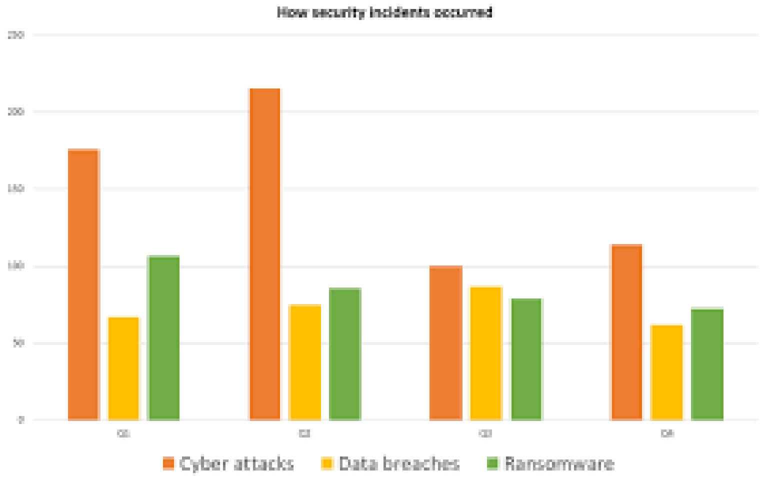
The above chart shows [5] far fewer incidents in the second half of the year, after COVID-19 restrictions eased in countries across the globe and people returned to the office. In the first 6 months of the year, we found 727 publicly disclosed security incidents. It was around this time that countries across Europe began lifting their restrictions. [5]

The UK celebrated **'Freedom Day'** on 19 July, with the end of social distancing and mask mandates, while similar decisions were made at state-level in the US.[5] These rulings coincided with a decrease in the number of data breaches in the second half of the year, as we discovered just 515 publicly disclosed incidents.[5]

V. ENCOUNTER OF SECURITY INCIDENTS

- In compilation our monthly lists, we tend to distinguish between breaches caused by 'data breaches' and people that result from 'cyber attacks'. [5]
- We also provide ransomware its own class, to some extent to the frequency of attacks and to differentiate it from intrusions that may harder to notice, like password breaches.[5]
- Separating security incidents in this way reveals additional concerning how they happen and who the concerned person to be blamed which is shown in the chart below[5]

Table: 5



Source: https://geekflare.com/database-threats-and-prevention-tools/

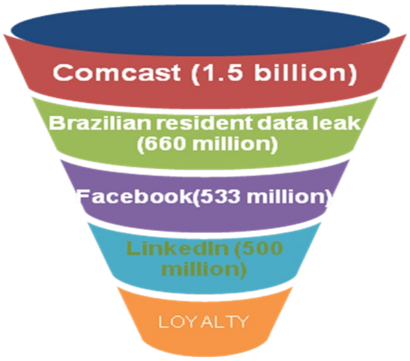
- Cyber attacks were the primary frequent form of security incident in 2021 – though this encompasses a broad range of threats. Criminal hackers were mostly focuses on organizations so that they could gain unauthorized access to a company account. [5]

- Of the incidents during which the supply of the breach was acknowledged, [5] 29% occurred as a results of unauthorized access. Phishing is one such attack vector, with fraudsters usually leverage their access to conduct ransom ware attacks. [5]
- When talking about ransom ware, we found 401 such incidents in 2021, and 39% increase over the previous year (289). [5]

VI. BIGGEST DATA BREACHES OF 2021

It is difficult to know exactly how many private records are negotiated each year, because few publicly disclosed incidents contain this information. However it was revealed 5,126,930,507 breached records.[5] The circumstances that resulted in the large number of breached records in 2021 were:

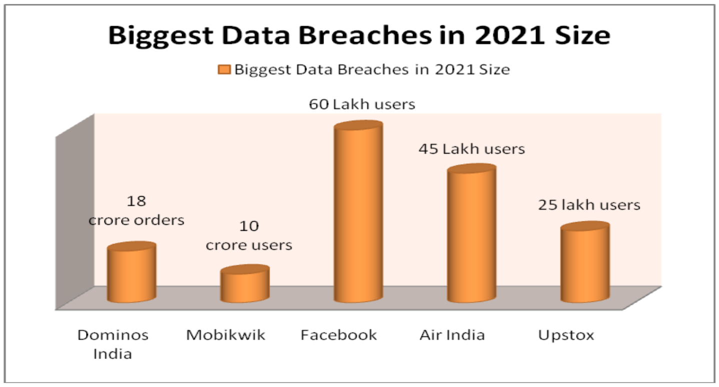
Table : 6



The LinkedIn breach, for example, comprised information scraped from people's public profiles. However, no financial records were affected, although attackers almost have used this information in scams designed to turn data into currency. But it is very difficult to say how successful they were.

i. Five major data breaches in India 2021

Table : 7



Source : https://www.91mobiles.com/hub/5-major-data-breaches-india2021/

ii. Top five nations targeted by hackers

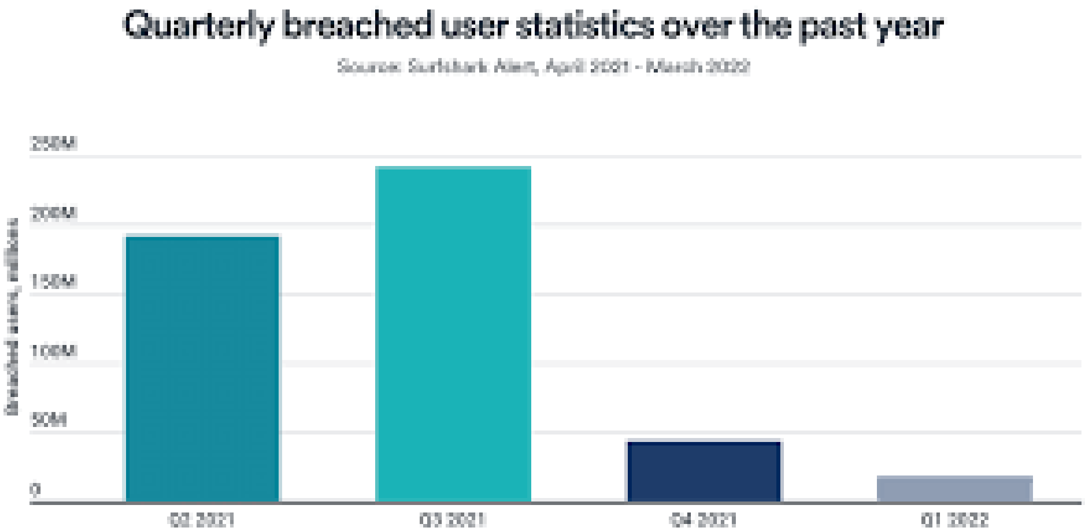
Even though there is 62% drop in data breaches, India is among the top five nations targeted by hackers

- Data breaches of Indian users could have fallen sixty two per cent this quarter than the last, however the country still remains among the highest 5 target nations for hackers, a study has found.[10]

- The study by Netherlands-based Virtual Private Network (VPN) supplier Surfshark open that 6,75,000 Indian users were breached this quarter whereas one.77 million users' information was hacked in this fall 2021.[9] **[10]**

- The survey found that the worldwide breaches had gone down by fifty eight per cent this quarter. golf shot it in numbers, that was 18,174,132 breaches in Q1, 2022 from 43,169,912 in Q4, 2021.[10]

Table : 8

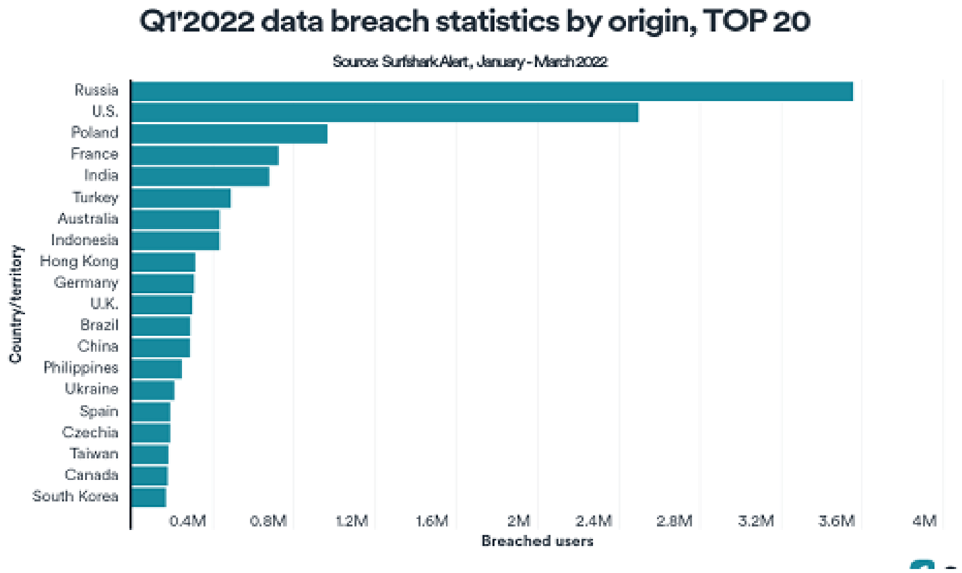


Source : Surfshark Alert, April 2021- March 2022

iii. Russia, US, Poland most breached nations

According to **Aleksandr Valentij, Chief Information Security Officer of Surfshark** "Data breaches remain one of the most common types of cybercrime, inspite of the decline it has demonstrated in the past months,"

Table : 9



Most breached countries of 2022
Source : Surfshark Alert, January- March 2022

- The above study shows that Russians made up almost a fifth of all global victims. In the month of March most of the hacking of Russian users went up by 11 per cent. According to the study, more than 3.5 million Russian internet users were targeted. [10]

- Around 136 per cent more Russian accounts were breached in March than in February.[10]

- The US is second on the list. The country had almost 50% fewer affected users than in the last, when 2.5 million users had been breached. [10]

- Poland, which took the third place, 514 per cent sharp spike in breaches with 961,000 users breached in the first quarter this year as compared to 159,000 last quarter. The country's media reported a wave of telephone phishing attacks at the beginning of the year, seeking to tempt out credit card details.[10]

- The findings of the data were collected for three months, between January to March 2022 (as Q1 2022), while the selected data was then analyzed and compared to the data from the previous quarter, from October to December 2021 (as Q4 2021). **[10]**

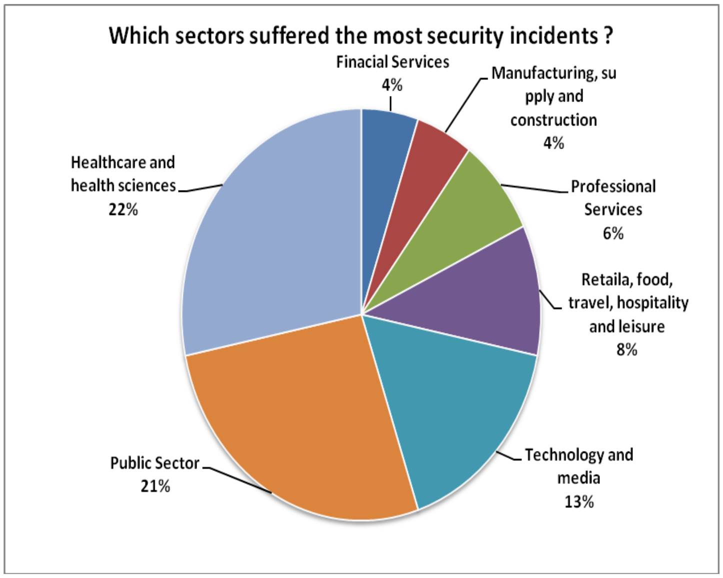
VII. THE MOST VULNERABLE SECTORS

The health sciences sector suffered the significant range of information breaches for the third consecutive year. It was recorded 277 incidents that accounted for 297 million breached records.

For example, betting on the character of the incident, tending breaches will reveal medical problems that may have an effect on victims' reputations.

Healthcare data can be used to carry out fraud, launch phishing attacks and, in some cases, reveal monetary information. The public sector was the opposite main contributor, accounting for 263 in public disclosed incidents. However, those breaches were larger on the average, with a complete of 794 million broken records. Despite being solely the fourth most broken sector, technology and media organizations were answerable for the prime breached records (1.8 billion). This is frequently largely due to large-scale breaches like those at Facebook and LinkedIn, that created up quite two- thirds of that total.

Table: 10



Source: Protect, Comply, Thrive, IT Governance Blog

VIII. EVALUATING SECURITY RISKS OF DATABASES IN 2022

In 2021, the highest average total cost of data breaches across the globe: **$4.24 million**[3]. Hacker attacks are getting more and more complex and sophisticated, and force businesses to bulletproof their database security standards.[3] Data breaches leads to harmful consequences and causes legal, financial, and reputational losses. Implementing regular and consistent database security checks will largely reduce the chances of a successful hacker attack. The main threats related with database security, as well as learn how to evaluate database risks and remove them. [3]

IX. SIX BEST PRACTICES FOR DATABASE SECURITY RISKS EALUATION

- To use separate servers
- To choose the HTTPS proxy server
- To stop using Default Network Ports
- To keep It Up To Date
- **To conduct backups**
- **To make use of database** firewalls**: There are three types of database firewalls**
    - Packet filter firewall
    - Stateful packet inspection (SPI)
    - Proxy server firewall

Finally, it is advisable to keep the firewalls up to date to avoid the newer methods of hacker attacks

X. TECHNIQUES AND STRATEGIES TO PROTECT DATABASES

To provide adequate protection for an organization's databases, a defensive matrix of best practices is required, combined with regular internal controls. The best practices matrix includes the subsequent terms:

- To manage user access rights and eliminates excessive privileges and inactive users.

- Need to train the workers on risk mitigation techniques, including recognizing common cyber threats like spear-phishing attacks, best practices around the Internet and email usage, and **password management**.
- To assess any information vulnerabilities, and to establish compromised endpoints and classify sensitive information.
- To monitor all the information access activity and usage patterns in real-time to in order to detect data leaks, unauthorized SQL and **Big Data** transactions, and protocol/system attacks.
- To automate auditing with an information protection and auditing platform.
- To block malicious web requests.
- To archive external data, **cyber databases,** and mask database fields to hide sensitive information.

XI. DATABASE SECURITY TOOLS

The above techniques requires a lot of effort for the organization's Information Technology department, and many times it so happen that the IT staff cannot keep up with all of their tasks, so to keep databases secure and are left undone. Therefore, a few tool can make these tasks easier so that the dangers that threaten databases do not affect them. They are

- **Scuba Database Vulnerability Scanner**
- **dbWatch Control Center**
- **AppDetectivePRO**
- **DbDefence**
- **OScanner**
  - Sid enumeration
  - Password testing (common and dictionary)
  - Oracle version enumeration
  - Enumeration of user account roles, privileges, and hashes[6]
  - Enumeration of audit information
  - Enumeration of password policies
  - Enumeration of database links
- **dbForge Security Manager**

XII. CONCLUSION

The conclusion of my study is that it is common for all the organizations to believe that their knowledge is only secured if they take backups and use firewalls. However there are several different aspect of information security that fall on the far side, those security measures. Whereas choosing a database server, the organization should take into account the security aspects that imply giving information servers the importance they need within the strategic management of associate degree organization's vital knowledge. If the user recognize vulnerabilities and problems in information security and take action to get rid of or mitigate them, cyber attacks won't be as damaging. Users and business firms are finally getting aware of the importance of having strong protective algorithms, and a professional safety team. Therefore if planning on building software or already have a site or app, make sure the database is safe and revisit your information-handling practices

References

[1] Rathore Sneh, Sharma Anupama, Department of Information Technology, HMR Institute of Techology, New Delhi, India, International Journal of Engineering Research & Technology IJERT), Proceedings Database Security- Attacks, Threats and Challenges ISSN:2278-0181, ICCS-2017 Conference (accessed on 21.04.2022). https://www.ijert.org/database-security-attacks-threats-and-challenges

[2] Understanding Comprehensive Database Security – Technical White paper Rimini. https://www.riministreet.com/wp-content/uploads/2020/07/Rimini-Street-White-Paper-Understanding-Comprehensive-Database-Security.pdf. (accessed on 21.04.2022)

[3] Joshua Otwell, December 1, 2021, Digital Owl's Prose Sql and PHP Developer diaries https://joshuaotwell.com/evaluating-security-risks-of-databases-in-2022/

[4] https://informationsecurity.report/Resources/Whitepapers/e763d022-6ee4-4215-9efd 1896b0d9c381_wp_topten_database_threats%20imperva.pdf

[5] Luke Irwin, 20th January 2022 Protect, Comply, Thrive, IT Governance Blog, https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2021-5-1-billion-breached-records

[6] The Most Dangerous Database Threats and How to Prevent Them By Geekflare Editorial in Security on January 8, 2022. https://geekflare.com/database-threats-and-prevention-tools/

[7] Database Security: An Essential Guide By IBM Cloud Education, 27 August 2019. https://www.ibm.com/cloud/learn/database-security Learn Hub

[8] Database security policies.docx - Controls and policies In...Sario,Act 1.docx – ACTIVITY 1 Yna C. Sario 2-DOMT 1 1. Key...https://www.coursehero.com/file/83881995/Database security-policiesdocx/

[9] aljazeera.co.in › politics › despite-62-drop-in-dataDespite 62% drop in data breaches, India among top 5 nations. https://aljazeera.co.in/politics/despite-62-drop-in-data-breaches-india-among-top-5-nations-targeted-by-hackers-study-finds//

[10] theprint.in › india › despite-62-drop-in-dataDespite 62% drop in data breaches, India among top 5 nations . https://theprint.in/india/despite-62-drop-in-data-breaches-india-among-top-5-nations-targeted-by-hackers-study-finds/917197//

[11] https://jelvix.com/blog/database-security

[12]https://openknowledge.worldbank.org/bitstream/handle/10986/24774/Ethiopia000Oil0ework 000final0report.txt?sequence=2