iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VIII **Month of publication:** August 2024

DOI: https://doi.org/10.22214/ijraset.2024.63853

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VIII Aug 2024- Available at www.ijraset.com

A Comparative Study on Database Breach and Security in Contemporary Perspective

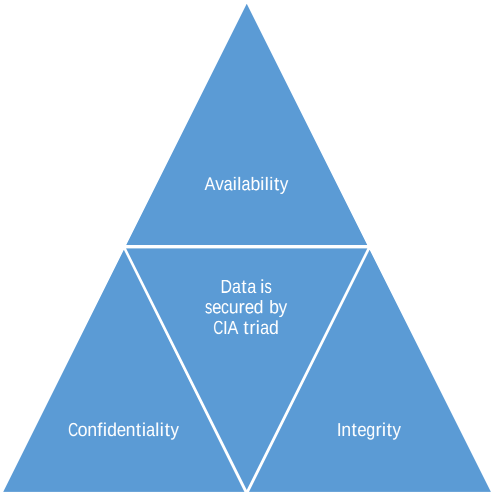
Shivani Sharma
Assistant Professor, Department of Computer Science Engineering, Himalayan School of Science and Technology, Swami Rama Himalayan University

Abstract: In the modern technical landscape, database security has emerged as a critical concern. The primary goal of database security is to prevent unauthorized access and data modification while ensuring uninterrupted access to required services. Various security measures have been devised to safeguard databases, and numerous security models have been established, each focusing on different aspects of database security. The effectiveness of these security measures relies on the design and development of the database management system for protection. In the current environment where web applications with databases as a backend are proliferating, a secure database management system is vital, going beyond just securing the database itself. This paper focuses on database breaches, identifying the risks, security measures, and weaknesses in managing a Database Management System.

Keywords: Data breach, database security challenges, database risk, Ransom ware, Breach cost

I. INTRODUCTION

Relational database systems have been adopted as the infrastructure for data repositories in recent years due to advancements in hardware capability and volume capacity, as well as extensive use of World Wide Web platforms and information systems. Due to the decentralized nature of information management, massive volumes of data and information are now a major source of security challenges. Relational database security concepts are frequently built on the CIA triangle of security, which refers to availability, integrity, and confidentiality. To ensure that the data is secure, these elements need to be included in the application processes [1]. Fraud and theft affect the database environment, which in turn affects the entire company. Although the data itself is not being altered, the integrity and privacy may be compromised. The term "confidentiality" relates to keeping material secret, usually only when it's essential to the company. Loss of privacy and competitiveness may follow security lapses that cause confidentiality to be compromised. When data integrity is compromised, it becomes tampered with and altered. Many businesses are looking for what is known as "24/7" availability, or availability that is available for use twenty-four hours a day, seven days a week. When there is a loss of availability, either the data or the system cannot be accessed. As a result, the goal of relational database management systems is to minimize losses brought on by dangers or unforeseen circumstances. A threat is an instance or circumstance that could have a negative impact on an organization's systems. To find and identify the most dangerous risks, the organization needs to put in time and effort [1, 2, 3].



II. DATABASE SECURITY CHALLENGES

The database can be viewed at three various levels of abstraction. Usually, a three-level perspective is introduced, including an internal dimension, representing the physical storage of the database and the physical processing of the data, A logical (or conceptual level) level that provides users with a high level explanation of the physical world that the database represents; and an objective level (or view level) that defines the views that various users or programs have on the storage data. Just section of the entire database is defined at this point. The internal dimension maps the abstract structures provided by the data model to the actual structures in the underlying operating system. In addition to access and processing facilities, each DBMS must also have security measures to ensure confidentiality, honesty and accessibility of data stored[7, 12].

This is a common practice for organizations to protect the enterprise at the level of the network, as a rational approach because all risks are external. However, according to CERT's annual report, up to 50% of the network attacks come from inside. In fact, that's why many organizations are implementing a second protection level made up of point-of-the-art technologies that secure databases. In the case of data privacy against security attacks, the quality of the data is perceived to be an indicator of the value given to the data by its user. There are several reasons to identify data responsiveness [12].

1) The meaning of a data itself can be so exposing or secret that it is vulnerable.
2) The origins of a data might suggest the need for confidentiality.
3) The specific trait or record could have been considered to be vulnerable.
4) Any data will not be vulnerable on its own, but may become vulnerable in the presence of any other data.

The details and the general cyber management issues are the main aspects of technology that have a significant effect on businesses today. Server protection can be exposed to danger by accessing confidential data, modifying data, etc.

Degrading the functionality of the website or doing serious harm to the credibility of the client and industry. Each IT system must be categorized according to the most important data collected, interpreted or distributed by the IT system[9, 11].

III. DATABASE SECURITY CHALLENGES

The database can be viewed at three various levels of abstraction. Usually, a three-level perspective is introduced, including an internal dimension, representing the physical storage of the database and the physical processing of the data, A logical (or conceptual level) level that provides users with a high level explanation of the physical world that the database represents; and an objective level (or view level) that defines the views that various users or programs have on the storage data. Just section of the entire database is defined at this point. The internal dimension maps the abstract structures provided by the data model to the actual structures in the underlying operating system. In addition to access and processing facilities, each DBMS must also have security measures to ensure confidentiality, honesty and accessibility of data stored [4, 7]. This is a common practice for organizations to protect the enterprise at the level of the network, as a rational approach because all risks are external. However, according to CERT's annual report, up to 50% of the network attacks come from inside. In fact, that's why many organizations are implementing a second protection level made up of point-of-the-art technologies that secure databases. In the case of data privacy against security attacks, the quality of the data is perceived to be an indicator of the value given to the data by its user. There are several reasons to identify data responsiveness [7]. The meaning of a data itself can be so exposing or secret that it is vulnerable. The origins of a data might suggest the need for confidentiality. The specific trait or record could have been considered to be vulnerable. Any data will not be vulnerable on its own, but may become vulnerable in the presence of any other data. The details and the general cyber management issues are the main aspects of technology that have a significant effect on businesses today. Server protection can be exposed to danger by accessing confidential data, modifying data, etc. Degrading the functionality of the website or doing serious harm to the credibility of the client and industry. Each IT system must be categorized according to the most important data collected, interpreted or distributed by the IT system [5, 6].

A. SQL Injections

Database systems are used for the backend functionality. User supplied data as input is often used to dynamically build SQL statements that affect directly to the databases. Input injection is an attack that is aimed at subverting the original intent of the application by submitting attacker – supplied sql statements directly to the backend database.[9] There are two types of input injection:

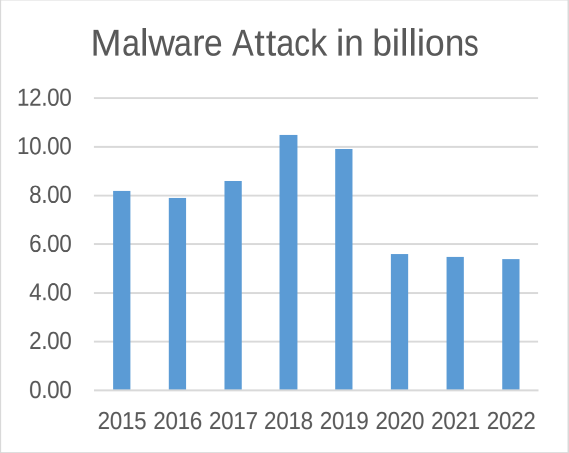
1) *SQL Injection:* Targets the tradition database system. It attacks usually involve injecting unauthorized statements into the input fields of applications.
2) *NoSQL Injection:* Targets big data platforms. This type involves inserting malicious statements into big data components like Hive, MapReduce.

Some action to reduce the effect:

- We can use pre-processed statements instead of direct queries.
- We can apply MVC pattern.

B. Malware

Cybercriminals, state-sponsored hackers, and spies use advanced attacks that blend multiple tactics – such as spear phishing emails and malware – to penetrate organizations and steal sensitive data. Unaware that malware has infected their device; legitimate users become a conduit for these groups to access your networks and sensitive data.



Some action to reduce the effect:

- It is suggested that a stringent access and privilege management policy be enforced and maintained.
- Do not provide client staff excessive rights and revoke expired rights in time.

C. Backup Exposure

Backup storage media is often completely unprotected from attack. As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect backup copies of sensitive data and monitor your most highly privileged users is not only a data security best practice, but also mandated by many regulations.

D. Weak Authentication

Weak authentication schemes allow attackers to assume the identity of legitimate database users. Specific attack strategies include brute force attacks, social engineering, and so on. Implementation of passwords or two-factor authentication is a must. For scalability and ease-of-use, authentication mechanisms should be integrated with enterprise directory/user management infrastructures.

1) Backup Exposure

Backup storage media is often completely unprotected from attack. As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect backup copies of sensitive data and monitor your most highly privileged users is not only a data security best practice, but also mandated by many regulations.

2) Some Action to Reduce the Effect

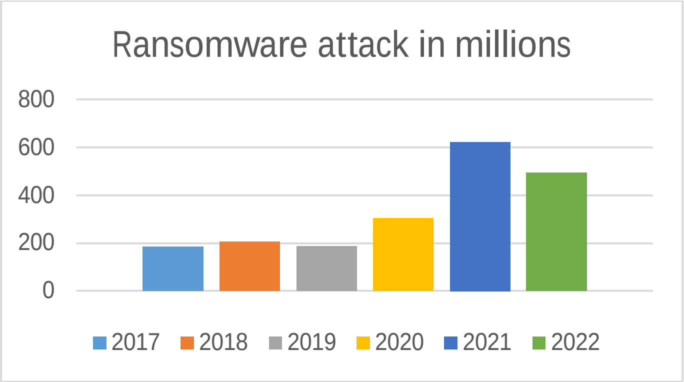
Use strong authentication methods, such as two-factor mobile authentication, passwords, and biometrics. If no other authentication methods are open, enforce strict username/password policies.[8]

IV. A FEW 2023 DATA BREACH INCIDENTS IN INDIA

X (Twitter): For a number of years, Twitter has been accused of data breaches. This year, the website also had a similar occurrence. A dark web database containing the email addresses of almost 200 million individuals could be purchased for about $2. According to BleepingComputer since July 22nd, 2022, threat actors and data breach collectors have started selling and distributing enormous data sets of scraped Twitter user profiles comprising both private (phone numbers and email addresses) and public data on different online hacker forums and cybercrime markets.

By taking advantage of a Twitter API flaw that let users enter phone numbers and email addresses to find out if they were linked to a Twitter ID, these data sets were produced in 2021. Then, using a different API, the threat actors scraped public Twitter data for the ID. They then blended the public data with private phone numbers and email addresses to build Twitter user profiles.

1) *ChatGPT:* An error in the open-source library of ChatGPT resulted in the unintentional disclosure of user information, including conversation titles and partial credit card numbers. OpenAI quickly fixed the problem by pulling ChatGPT down. Users may view certain personal information of others, including names, email addresses, payment addresses, and partial credit card information, while the system was exposed.
2) *MSI:* Popular computer retailer MSI was the target of a ransom ware assault that claimed to have stolen 1.5TB of data from MSI's servers, including firmware, secret keys, and source code. The hack caused financial losses for MSI. They threatened to make the stolen material public if they did not get their $4 million ransom requested.
3) *SONY:* A ransom ware organization attacked Sony, stealing over 6,000 files, including Java files and build logs that might be used to create exploits for Sony systems. If their demands for ransom are not fulfilled, the attackers threatened to put the stolen data up for sale.



A SUMMARY OF DATA BREACHES

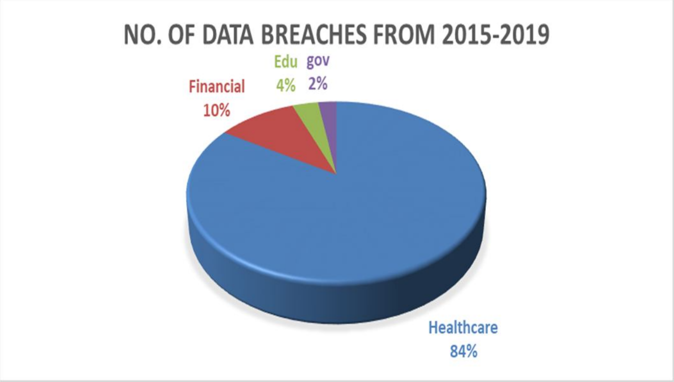
Company	year	Affected Data records	Estimated Cost for lost data
X (Twitter)	2023	200 million customers' records	$400 million
ChatGPT	2023	unknown	unknown
MSI	2023	1.5 TB	$400 million
SONY	2023	6000 files	unknown

V. ANALYSIS OF DATA BREACHES ACCORDING TO SECTORS FROM 2015-2019

Data breaches have the potential to cause harm to both individuals and organizations in various ways. In addition to the significant financial losses that organizations experience as a result of data theft, such incidents also have a negative impact on the organizations' reputation and brand value. Data breaches are commonly divided into two main categories: internal and external. Internal data breaches encompass incidents that involve an internal agent. These may include privilege abuse, unauthorized access/disclosure, improper disposal of sensitive data, loss or theft, or accidental sharing of confidential healthcare data with unauthorized parties. External data breaches are incidents caused by an external entity or source. 1. This includes any incidents related to hacking or information technology, such as ransomware, phishing, spyware, malware attacks, and credit card fraud.

The Privacy Rights Clearinghouse (PRC), a non-profit organization located in the United States, disclosed that between January 2005 and October 2019, there were 9,016 reported data breaches across multiple industries. In total, over 10 billion records (10,376,741,867) were compromised due to these breaches [10]. The PRC database features reports on several data breach occurrences pertinent to each sector. Since no records were compromised during certain intrusions, the authors have omitted those figures from their analysis concerning the depiction of data breaches by sector. After an exhaustive analysis of the PRC database, the compiled information was tabulated in Table

Name of the sector	No. of data breaches from 2015-2019
Healthcare	1587
Financial	194
Educational	64
government	45

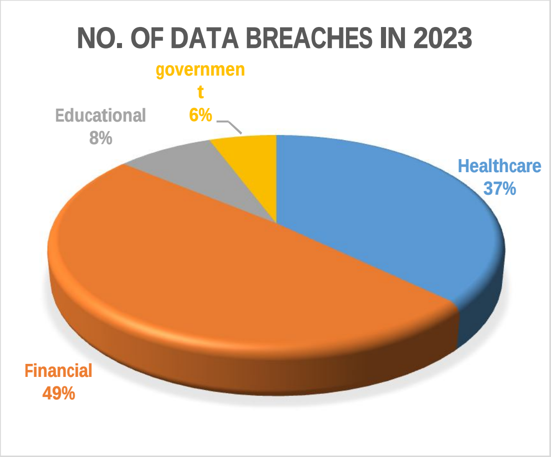


VI. ANALYSIS OF DATA BREACHES ACCORDING TO SECTORS IN 2023

During the initial quarter of 2023, a total of 6.41 million data records were compromised in global data breaches, affecting millions of people. The exposure of confidential data can lead to significant financial losses for businesses annually. On average, a single compromised data record amounted to $165 in 2023. In contrast, the average cost of a data breach incident for companies worldwide was $4.45 million, encompassing expenses related to detection, operational disruptions, post-incident actions, and notifications. Notably, the most expensive phase of a data breach was the identification and containment of the breach.

Cybercriminals typically aim to access highly sensitive data. In 2023, over half of all data breaches in global enterprises involved customer personally identifiable information (PII), making it the most commonly compromised data category. Approximately 40% of data breaches included employee PII. Additionally, 76% of social engineering attacks led to the exposure of login credentials, with financial and insurance firms being the most targeted industries for credential theft.[11][12]

Name of the sector	No. of data breaches in 2023
Healthcare	1080
Financial	1422
Educational	239
government	166



Name of the industry	Number of Compromises in 2023	Average cost of Data Breach
Healthcare	809	$10.93M
Financial	744	$5.9M
Educational	173	$3.65M
Professional	308	$4.47M

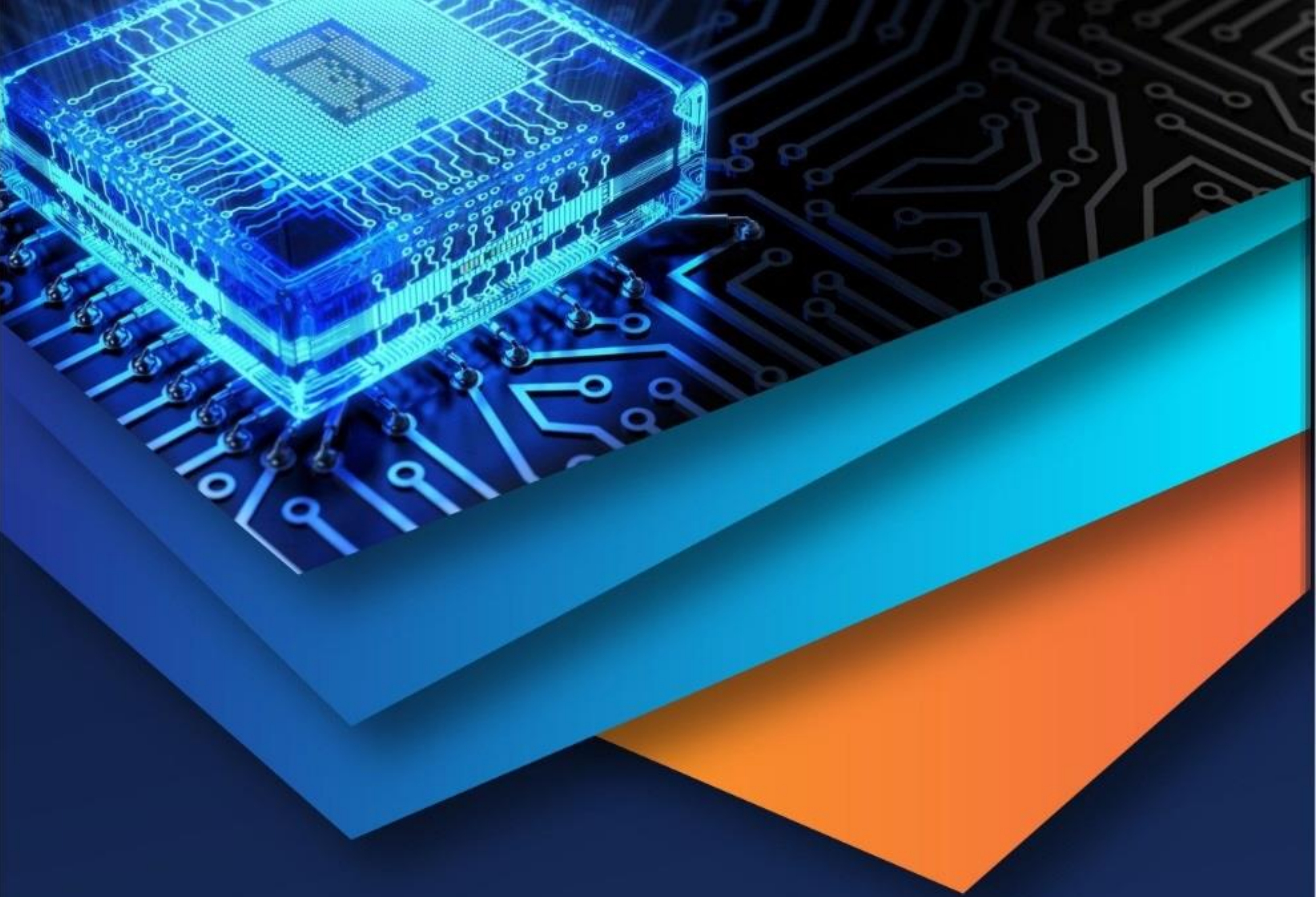
Source: (Identity Theft Resource Center, 2024)

VII. CONCLUSION

In our paper, we have outlined the types of data breaches, Challenges, and protection measures associated with database management systems. We have also seen that there is recognised hike in data breaches over the years. In the year 2023, Financial and healthcare institutions are the primary targets of data breach incidents. This is due to the fact that banks and insurance companies hold a large amount of sensitive data and financial assets, while healthcare institutions handle critical missions and collect sensitive information. We need further research to prevent data breaches as more data is made available electronically, it can be assumed that threats and vulnerabilities to the integrity of that data will increase as well.

REFERENCES

[1] T.Connolly, C. Begg. “Database Systems A Practical Approach to Design, Implementation, and Management”, 4th ed., Ed. England: Person Education Limited, 2005, pp. 542-547, 550-551.
[2] Almasri, O., & Jani, H. M. Introducing an Encryption Algorithm based on IDEA.
[3] Almasri, O., Jani, H. M., Ibrahim, Z., & Zughoul, O. (2013). Improving Security Measures of E-Learning Database. International Organization of Scientific Research-Journal of Computer Engineering (IOSR-JCE), 10(4), 55-62.
[4] M. Murray, Coffin, "Database Security: What Students Need to Know." Journal of Information Technology Education, vol. 9, pp 61-77, 2010.
[5] A. Furmanyuk, M. Karpinskyy and B. Borowik, "Modern Approaches to the Database Protection," 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, pp. 590-593, September 2007.
[6] P. B. Ambhore, B. B. Meshram, and V. B. Waghmare, "A Implementation of Object Oriented Database Security," 5th ACIS International Conference on Software Engineering Research, Management & Applications (SERA 2007), Busan,vol. 7, pp. 359-365, , 2007.
[7] Ş. Mariuţa, "Principles of security and integrity of databases." Procedia Economics and Finance, Targul din Vale, Romania, vol. 15, pp. 401-405, October 2014.
[8] ILO Somtoochukwu F., Ubochi Chibueze and Osondu U. S. “CORE THREATS AND PREVENTION IN DATABASE SECURITY” wjert, 2019, Vol. 5, Issue 3, 535-551.
[9] Mubina Malik and Trisha Patel, “DATABASE SECURITY - ATTACKS AND CONTROL METHODS”, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1, March 2016.
[10] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar and Raees Ahmad Khan, “Healthcare Data Breaches: Insights and Implications”, Healthcare (Basel). 2020 Jun; 8(2): 133.Published online 2020 May 13.
[11] https://www.statista.com/topics/11610/data-breaches-worldwide/#topicOverview(Accessed on 30 July 2024)
[12] https://secureframe.com/blog/data-breach-statistics (Accessed on 30 July 2024)



10.22214/IJRASET

INDEX
COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY