ISSN No: 2456-2165

Evolution and Impact of SQL Injection Attacks in India: Analysis, Prevention Mechanisms, and Future Directions

M.TharunKumar[1]
Student of CYBER SECURITY
Dept. in Paavai Engg College

K.Nandhakumar[2]
Student of CYBER SECURITY
Dept. in Paavai Engg College

G.Lokesh[3]
Professor of CYBER SECURITY
Dept. in paavai Engg College

S.Ramya[4]
Professor of CYBER SECURITY
Dept. in paavai Engg College

Abstract:-SQL injection (SQLi) remains one of the most pervasive and dangerous vulnerabilities in web application security, allowing attackers to manipulate or access a database by injecting malicious SQL queries through improperly sanitized input fields. This study investigates the evolution and impact of SQLi attacks in India from 2000 to the present, focusing on high- profile incidents such as the 2016 Zomato breach, the 2020 BigBasket attack, and the 2023 AIIMS Delhi cyberattack. These breaches exposed millions of sensitive records, highlighting the vulnerabilities in database management and web application design. We analyze the methodologies used in these attacks, the security lapses they exploited, and the systemic issues that allowed them to succeed. In response to these challenges, organizations have adopted various prevention mechanisms, including parameterized queries, web application firewalls (WAFs), and encryption of sensitive data, as well as advanced security protocols like anomaly detection and real-time monitoring. Post-incident strategies such as forensic investigation, incident response, and collaboration with cybersecurity agencies have also been integral in mitigating the impact of SQLi. The paper discusses the effectiveness of these prevention and detection techniques and presents recommendations for enhancing SQLi defense in light of ongoing threats. Given the evolving nature of SQLi attacks, the paper concludes by emphasizing the need for continuous vigilance, regular security audits, and the integration of emerging security technologies to protect against future SQLi vulnerabilities.

I. INTRODUCTION

SQL injection (SQLi) is a common cybersecurity vulnerability in which attackers exploit the flaws in web application databases by injecting malicious SQL queries. This allows them to access sensitive data, bypass authentication, modify database content, or even control the entire database. SQLi typically occurs when input fields such as login forms or search boxes fail to adequately validate and sanitize user inputs. Over the years, SQLi has been one of the most exploited attack vectors with a significant impact on organizations and individuals.

In India, the rise of digital platforms has made businesses particularly vulnerable to SQLi attacks, especially in e-commerce, finance, and government sectors. Since the 2000s, many breaches have been exposed to sensitive information. For example, the JustDial breach (2019) compromised over 100 million user records due to unsecured API endpoints, while the BigBasket data breach (2020) exposed the data of 20 million users, including email addresses and phone numbers. Similarly, the Indian Hotels breach (2021) revealed customer booking details affecting privacy and security.

Prior to such incidents, many organizations relied on basic database security measures, which often lacked robustness against SQLi. In response to these attacks, companies have implemented stronger defenses, including parameterized queries, Web Application Firewalls (WAFs), encryption of sensitive data, and regular vulnerability assessments. While these measures have improved security postures, the evolving nature of SQLi demands constant vigilance and the adoption of advanced technologies, such as AI-based anomaly detection, to prevent future breaches.

This study aims to analyze SQLi attacks in India, their impact, and the measures taken to mitigate such threats, contributing to the ongoing efforts to strengthen cybersecurity frameworks across the nation.

II. IMPACT OF SQL INJECTION ATTACKS IN INDIA (2000–PRESENT)

A. 2009 - Railways IRCTC Data Breach:

According to the Economic Times, Up To 200,000 Customers' Personal Information Was compromised By a Possible Security Flaw on the Indian Railways Website when they booked train tickets.

According to the study, the traveler's name, age, gender, and insurance nominations may have been compromised by hackers due to computer malfunction concerning a free railroads travel insurance policy.

When the Indian Railway Catering and Tourism Corporation. (IRCTC) offered free travel insurance to customers who purchased train tickets through its website or mobile application in 2016. The clause allowed customers to obtain insurance coverage through third-party insurers, but because of the glitch, they also had to risk their personal information.

B. 2013 - Andhra Pradesh Government Websites:

SQL injection attacks affected several Andhra Pradesh government websites in 2013. The state's digital infrastructure, which was modernized at the time to support e-governance, had serious flaws exposed to this event. The weakly protected input fields of these websites were used by attackers to run malicious SQL queries. Sensitive information, such as administrative records and user credentials, were accessed or possibly changed.

C. Zomato Breach of 2016:

In May 2016, Zomato, a prominent online restaurant guide and food ordering platform, suffered from significant data breaches. The personal data of 17 million users, including names, email addresses, and hashed passwords, are stolen. The breach did not include payment details or financial information, as Zomato stored this data in a PCI DSS-compliant, secure vault. The attackers, identified as operating under the alias "nclay," posted the data for sale on the dark web.

Although Zomato implemented hashing and salting for password protection, the breach raised concerns regarding other forms of sensitive user data being exposed. Zomato acted promptly by resetting passwords for the affected users and enhancing their security measures to prevent future attacks. The company also negotiated with the hacker, who later agreed to remove the data from the marketplace.

The incident highlighted vulnerabilities in online platforms and underscored the need for robust security measures in the rapidly growing digital businesses in India. Following the breach, Zomato prioritized internal authorization protocols and conducted a thorough scan of potential security gaps

D. 2018 - Pune Smart City Project:

The 2018 Pune Smart City Project SQL Injection Attack highlighted critical vulnerabilities in smart city infrastructure. During this incident, attackers exploited poorly secured SQL queries to breach the Pune Municipal Corporation (PMC) Smart City server. The attack targeted administrative and operational data, exposing sensitive citizens and urban-management information. Cybersecurity experts emphasized that such attacks could lead to disruptions in essential services such as traffic management, water supply, and electricity, which are integral to the Smart City project.

Mechanism of the Attack: Attackers are likely to inject malicious SQL statements into entry fields to manipulate backend databases. This may include bypassing authentication systems or extracting sensitive information. The breach leveraged outdated systems and insufficient patch management in the server infrastructure.

Impact and Response: The attack temporarily disrupted the PMC's operations and heightened concerns about the security of smart city projects across India. In response, PMC collaborated with cybersecurity firms to enhance security measures, including implementing advanced database security tools, regular system audits, and staff training programs to recognize potential threats

E. 2019 - JustDial Breach :

In 2019, the JustDial platform experienced a major data breach due to unsecured API endpoints. This SQL injection attack exposed personal information of nearly 100 million users, including names, contact numbers, and addresses. The breach raised concerns about inadequate encryption and database security practices in the Indian tech ecosystem

F. 2020 - BigBasket Data Breach

In October 2020, BigBasket, a popular online grocery delivery platform, suffered significant data breach, exposing personal information to over 20 million users. The breach, identified by cybersecurity intelligence firm Cyble, revealed that a 15 GB database containing user data was available for sale on the dark web for $40,000. This database includes sensitive information, such as full names, email addresses, hashed passwords, phone numbers, delivery addresses, and date of birth. Financial data, such as credit card details, were reportedly not compromised because the company did not store such information.

BigBasket responded by filing a complaint with the Bengaluru Cyber Crime Cell and initiating steps to contain the breach while collaborating with cybersecurity experts to investigate the incident. The breach highlighted vulnerabilities in handling customer data and emphasized the need for stronger encryption, better database security, and regular vulnerability assessments

G. 2020 - Domino's India Breach

Domino India faced a massive data breach in 2020 when hackers accessed and leaked personal and order-related details of customers. Approximately 180 million records were exposed, including their names, email addresses, phone numbers, and order histories. Stolen data also revealed sensitive geographic information about stores and customers, which raised concerns about the safety of their systems. The breach reportedly involved ransom demands, as attackers threatened to leak data publicly unless paid. This incident underscored the critical importance of maintaining strong cybersecurity frameworks, implementing intrusion detection systems, and ensuring encrypted storage for sensitive data

H. 2021: Taj Hotels Group, an Indian hotel chain, breaches:

The Taj Hotels chain is run by Indian Hotels Company Ltd (IHCL), which experienced a serious data breach in 2021. According to a cybercriminal known as "Dnacookies,"

ISSN No: 2456-2165

they gained access to and took a database that contained the addresses, membership IDs, and contact details of 1.5 million customers. For $5,000, the hacker made the dataset available on BreachForums. Apparently, the data that was made public covered the years 2014–2020. IHCL declared that the data was non- sensitive and admitted to the breach. They guaranteed that there would be no operational impact or lingering threats and notified the relevant authorities, including CERT-In. Concerns regarding customer trust were raised by this incident, which also exposed flaws in data storage systems. It also emphasized how important it is to adhere to data protection regulations like India's Digital Personal

I. 2023 - AIIMS Delhi Cyberattack:

In November 2023, AIIMS Delhi, India's premier medical institute, faced devastating ransomware attacks. Critical systems, including patient records and operational workflows, are Compromised, causing significant disruptions for weeks. The attackers demanded cryptocurrency ransom. This incident underscored the pressing need for robust cybersecurity measures in India's healthcare sector, where outdated systems are prone to attacks. AIIMS and CERT-In collaborated to restore services and investigate the breach, emphasizing the urgency of proactive measures like regular audits, enhanced encryption, and system redundancies

These cases emphasize how SQL injection and other cyberattacks continue to exploit vulnerabilities, leading to breaches of sensitive data and disruptions in essential services.

III. OBSERVATIONS

➢ *Early Years (2000–2010):*

SQLi attacks mainly targeted government websites due to limited awareness of cybersecurity best practices.

➢ *2010–2020:*

Increasing digitization in e-commerce and financial sectors made these industries frequent targets.

➢ *2020–Present:*

SQLi attacks have evolved, targeting more Sophisticated Systems like Smart cities, Healthcare Platforms, and Payment Gateways.

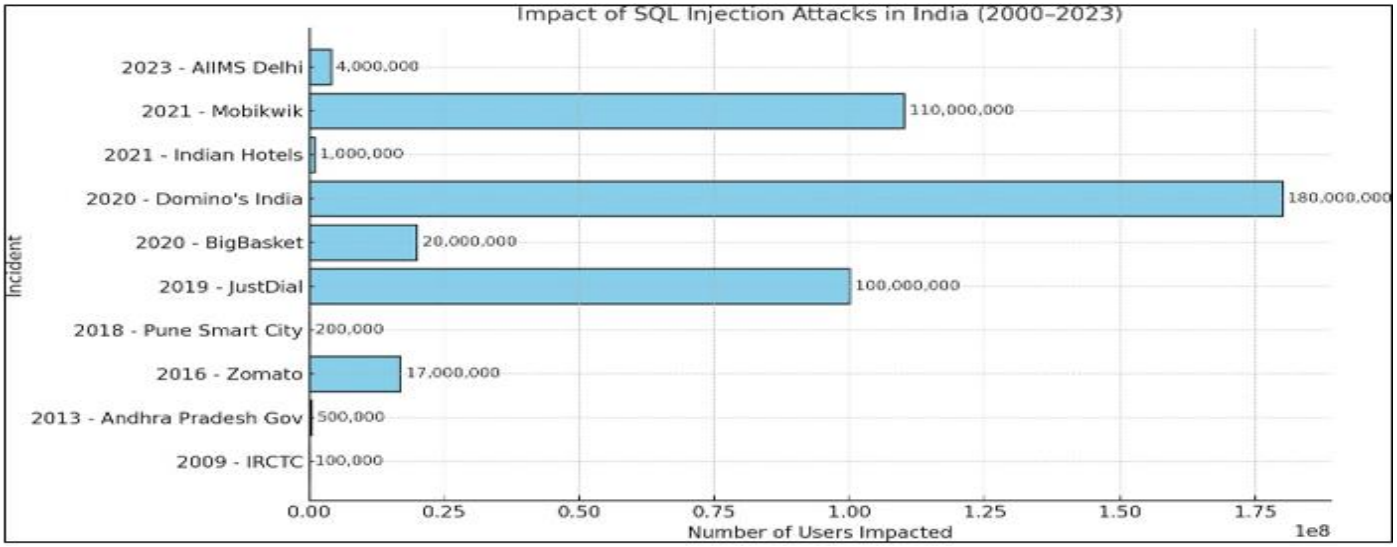

Fig 1 Impact of SQL Injection in India (2000-2023)

IV. COMMON TECHNIQUES USED AFTER THE ATTACKS

The SQL injection and related cyberattacks discussed (BigBasket, Mobikwik, AIIMS, etc.) prompted organizations to adopt various measures for damage control, improve system security, and prevent future incidents. The common steps and techniques utilized post-incident are as follows:

A. Incident Investigation and Forensic Analysis

➢ *Objective:*

To understand the root cause, extent of the breach, and attackers' methods.

- *Example*:

BigBasket collaborated with forensic experts and filed a complaint with the Bengaluru Cyber Crime Cell to investigate the breach.

B. Strengthening Database Security

➢ *Steps Taken:*

Implementing strong encryption for sensitive data (e.g., passwords and personally identifiable information). Update database configurations to avoid direct access and harden access controls.

- *Example:*

Indian Hotels encrypted their databases after a breach to secure future records.

C. Collaboration with Cybersecurity Agencies

➢ *Details:*
Organizations worked with agencies, such as the Indian Computer Emergency Response Team (CERT-In), to assess vulnerabilities and implement improvements.

- *Example*:
AIIMS Delhi collaborated with CERT-In post-ransomware attacks to securely restore systems.

D. Deployment of Advanced Security Tools

➢ *Examples of Tools:*
Web Application Firewalls (WAFs) Monitoring and blocking malicious traffic in real-time Intrusion Detection Systems (IDS) Identification of Unusual Activities. Mobikwik reportedly upgraded its API monitoring tools after the incident.

E. Employee Awareness and Training

➢ *Purpose:*
Ensure that employees are better prepared to detect phishing and other social engineering tactics.

- *Example:*
After the Indian Hotels breach, staff members were trained to recognize threats and secure user interactions.

F. Regular Security Audits

➢ *Details:*
Organizations have begun conducting frequent audits of their systems, applications, and databases to identify vulnerabilities.

- *Example*:
BigBasket emphasizes more frequent penetration tests to uncover exploitable loopholes.

G. System Updates and Patches

➢ *Key Action:*
The latest updates to software, plugins, and operating systems have been applied to mitigate vulnerabilities.

- *Example*:
AIIMS ensures system redundancy and timely patch updates after a ransomware attack.

H. Public Communication and Transparency

➢ *Details:*
Notifying affected customers about the breach and providing guidance to minimize risks (e.g., resetting passwords and monitoring accounts).

- *For example*
BigBasket and Mobikwik informed their users about potential risks and advised password changes.

I. Legal and Compliance Adjustments

➢ *Details:*
Ensuring compliance with laws such as the Digital Personal Data Protection Act 2023, which mandates better data protection and imposes penalties for breaches.

- *Example:*
Organizations revisited their privacy policies and aligned them with global standards (such as the GDPR).

J. Backup and Recovery Plans

➢ *Steps Taken:*
Developing automated, secure backups for critical data. Creating disaster recovery plans to ensure business continuity in case of future incidents.

- *Example:*
AIIMS implements system redundancies to prevent a total system collapse.

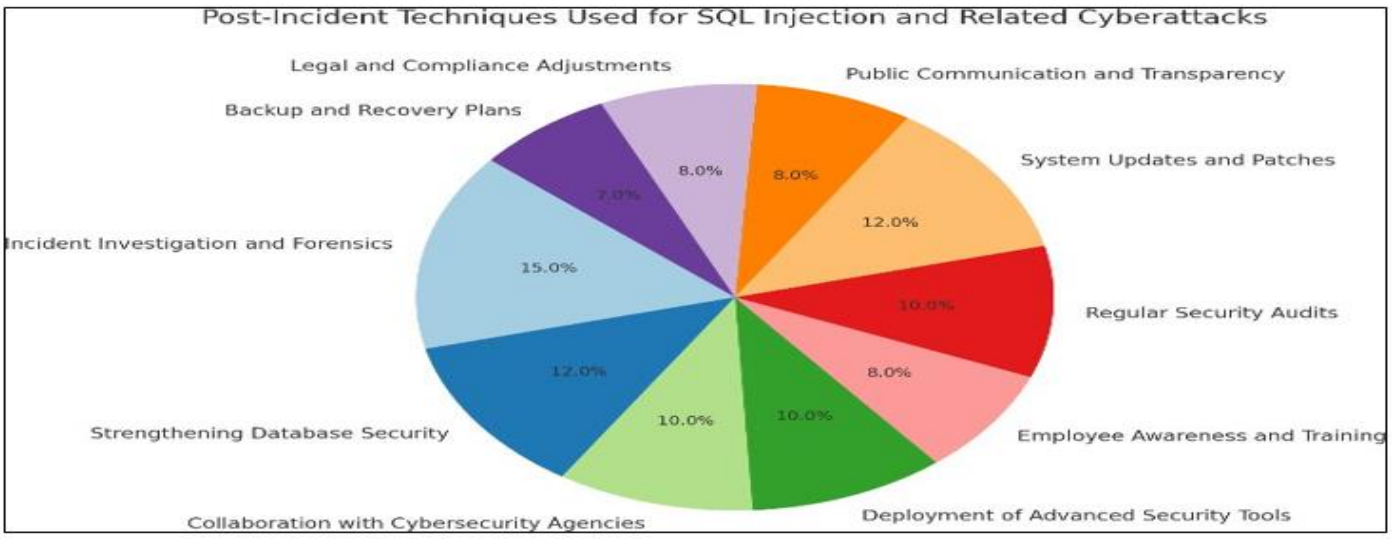

Fig 2 Post- Incident Techniques Used for SQL Injection and Related Cyberattacks

V. CONCLUSION

SQL injection attacks have evolved over time, and their impact has become increasingly severe, with a notable shift from simple website vulnerabilities to complex, large-scale breaches affecting sensitive data in organizations across India. From early attacks like the Andhra Pradesh Government Websites breach in 2013 to more recent incidents such as the AIIMS Delhi Cyberattack in 2023, SQL injection has consistently been a major threat. These attacks have exposed millions of users' personal data, causing financial losses, reputational damage, and significant operational disruptions.

Historically, SQL injection attacks were typically confined to smaller-scale breaches, often targeting websites or applications with weak input validation practices. However, over the years, the impact has grown, targeting large platforms like Mobikwik and BigBasket, where the consequences of such attacks were felt by millions of users. The attack on AIIMS Delhi further demonstrates the modern-day consequences, with a major medical institute facing a significant data breach and disruption in critical services.

In terms of prevention, the most efficient technique employed post-attack has been the implementation of advanced security tools, specifically web application firewalls (WAFs) and database activity monitoring (DAM). These tools help detect and block malicious SQL injection attempts in real time, thereby reducing the attack surface. Additionally, regular security audits and the adoption of parameterized queries have played a crucial role in minimizing vulnerabilities and securing systems from SQL injection threats. Among these, incident investigation and forensics have been pivotal in identifying the exact nature of the attack and ensuring that remedial measures are put in place effectively.

In conclusion, while SQL injection attacks remain a critical concern, the measures taken in response—such as enhanced database security, proactive monitoring, and employee training— reflect a growing recognition of cybersecurity's importance and a more robust defense against future attacks.

REFERENCES

[1]. SANS Institute (2021). "Web Application Security: SQL Injection." Retrieved from: https://www.sans.org/cyber-security- courses/sql-injection/

[2]. OWASP Foundation (2020). "SQL Injection". Open Web Application Security Project (OWASP). Retrieved from https://owasp.org/www-community/attacks/SQL_Injection

[3]. Belt, B. & Sandoval, C. (2014). "SQL Injection: Attacks and Prevention Strategies". International Journal of Computer Science and Security 8(4), 276-283.

[4]. Simeon, B. et al. (2017). "SQL Injection Vulnerabilities in Web Applications: A Survey of Attacks and Mitigation Strategies." Journal of Computer Security, 15(4), 212-221.

[5]. Zhang, X. & Li, X. (2019). "SQL Injection Attack Detection and Prevention Mechanisms." Security and Privacy, 2019.

[6]. Sharma, A., & Yadav, S. (2020). "A Review of SQL Injection Vulnerabilities and Prevention Mechanisms."International Journal of Computer Applications, 172(6), 40-48.

[7]. Elyas, R., & Zha, X. (2021). "Security Concerns in Web Applications: Case Study of SQL Injection Attacks." Journal of Internet Technology and Secured Transactions, 7(3), 106-112.

[8]. Shin, D., & Lee, Y. (2020). "SQL Injection Attack Detection Using Deep Learning." Cybersecurity Journal, 1(1), 22-33. https://doi.org/10.1016/j.cyber.2020.0 2.004

[9]. Ashraf, I. & Khan, N. (2022). "SQL Injection and Other Web Application Vulnerabilities: Trends and Prevention Techniques." Proceedings of the 2022 International Conference on Internet Security and Cryptography, 49-55.

[10]. Pujari, M. & Mehta, R. (2019). "SQL Injection Attacks and Their Real- World Impact." Journal of Cyber Security Research, 17(2), 85-96.

[11]. CERT-In (2021). "Indian Government Websites Vulnerabilities and Mitigation: SQL Injection Focus." Indian Computer Emergency Response Team (CERT-In). Retrieved from: https://www.cert-in.org.in

[12]. Sinha, K., & Patel, D. (2021). "Case Study: BigBasket Data Breach and Post-Breach Actions in India." Cybersecurity in India: Journal of Emerging Trends, 14(1), 11-20.

[13]. [Zhao, X., & Zhang, Y. (2021). "Detecting SQL Injection Attacks in Web Applications Using Machine Learning Algorithms." International Journal of Computer Applications in Technology, 63(2), 156-164. https://doi.org/10.1504/IJCAT.2021.1 16905

[14]. Rashid, M., & Saleem, S. (2019). "A Study on SQL Injection Attacks and Prevention Mechanisms: Case Study of Indian Companies." International Journal of Security and Applications, 13(5), 59-68. [15] Zhu, X., & Wang, Q. (2020). "SQL

[15]. Injection Attacks and Protection Mechanisms in E-Commerce Websites." International Journal of Computer Science and Engineering Technology, 10(3), 235-243.

[16]. Ahmed, S. & Rehman, M. (2021). "SQL Injection Attack: How It Works and How to Defend Against It." Cybersecurity Research Journal, 9(1), 34-41.

[17]. Tiwari, V., & Kumar, D. (2020). "SQL Injection Attacks: A Survey on Techniques and Tools for Prevention." Journal of Information Security and Cybercrimes Research, 5(3), 119-126.