A DEEP LOOK INTO CYBERSECURITY ISSUES IN INDIA: A REVIEW

Abstract

India had around 851 million internet connections as of the end of the financial year 2023. As a result, connectivity has increased by almost three times since 2015, when there were 302.33 million connections. Only 30% of Indians live in urban regions, but more connections in urban areas than in rural ones. Urban areas had 507 million internet connections as of 2023.
This work analyzed the crisis of cybercrime to highlighting the wide spread of cyberattacks occurred around the India. Study revealed the major attacks occurred in India. This work highlights the types of cyberattacks, data breaches occurred during the 2018 to 2022, penetration and security tools and Security measures to prevent cyber-attacks.

Keywords: - Security, attacks, cybercrime, Data Breach, Security tools, penetrating tools.

Authors

R Lakshman Naik
Depatment of CSE
Indian Institute of Information Technology
Sonepat, Haryana, India

Dr. Sourabh Jain
Depatment of CSE
Indian Institute of Information Technology
Sonepat, Haryana, India

Rajendra Prasad M
Depatment of CSE
Indian Institute of Information Technology
Sonepat, Haryana, India

I. INTRODUCTION

In 1960, only the military members, the researchers and scientists were accessed the internent. The number of Internet users has increased exponentially. In 1970s, computer crime means physical theft of computers and associated parts of it. When it comes to 1980s it is improved to viruses; it means intentionally making computers malfunction by inserting malicious software in to it. The impact was not as pervasive up until that point since internet use was restricted to research communities, big international corporations, and defence establishments. In 1996, the internent was first made ut available to the general public, verly fastly it got popularity among the people and gradually it altered their daily way of life.

Due to the introduction of GUI programing, usage of internet users was increased. The GUI programming provided user friendly environment to users to click the hyperlinks and to provide appropriate fields to provide desired information without worrying about data storage, way of data transmission over internet, tampering of data or snooped data over internet.

Instead of only breaking into computers, erasing data, or altering them for one's own gain, financial crime has become the main emphasis of computer crime. These cyber-attacks are multiplying quickly. In the year 2013, the cyberattacks impacted 800 million people and for every second around 25 computers were fallen prey to them. The CERT-India revealed that in the years 2011 to 2013 308371 Indian websites were compromised. It is also predicted that the annual loss was $160 million due to the cybercrim e and the mojority of cases were not recorded.

The Ministry of Communication and Information Technology submitted the 2013-14 report of standing committee about Information Technology to the 15th Lok Sabha shown the predicted information that is by the end of 2011year 100 million people were using internet and the number is rapidly increasing. There are currently about 134 major ISPs (Internet service providers) operating 22 million broadband connections in India.

India had around 851 million internet connections as of the end of the financial year 2023. As a result, connectivity has increased by almost three times since 2015, when there were 302.33 million connections. Only 30% of Indians live in urban regions, but more connections in urban areas than in rural ones. Urban areas had 507 million internet connections as of 2023 [3].

Please describe the nature of the cybercrime before we continue. The phrase "cyber crime" means any illegal behaviour that uses computing devices or computers, like stand-alone or networked cellphones, tablets, Personal Digital Assistants (PDAs), etc. as a tool or as a target. For the sake of money or out of retalation or adventure, people with criminal or destructive mindset frequently commit cybercrime.

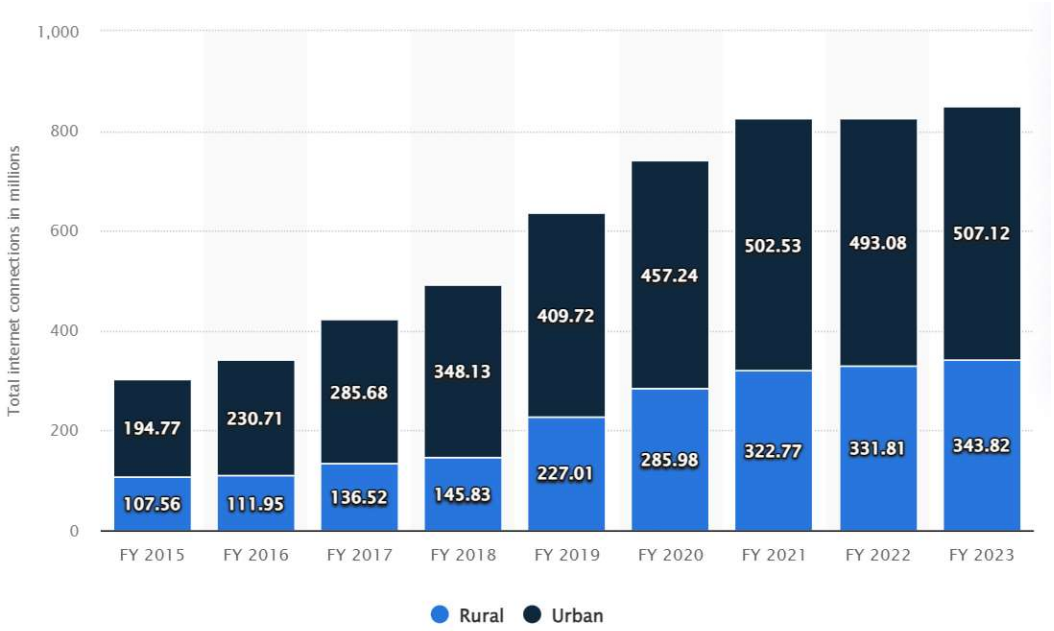

Figure 1

Cybercriminals can be either internal or external to the organization to do cyberattacks. Due to this the cybercrime classified into two categories as following:

1. **Insider Attack:** An insider attack committed by a user with authorized system access and attacks a computer system and network. Mostly, insider attacks committed by contractors or by unsatisfied internal employees. The main moto of this is because of greed or retaliation. The insider attacker well-aware of IT architecture, procedures, the security systems rules and flaws, he may easily carry out a cyber-attack. Because of it an insider attacker easily brings down the network and steal important data.

2. **External Attack:** This type of attackers may be employed by an inside or external party to the organization. The target of this cyber-attack is not only for reputational damage or but also for financial loss. As this type of attacker's outsiders of an organization, they often scan and still the data.

   A cyber-attack means an attack initiated from one or more computers against a network or a computer or a group of computers. The cyber-attacks divided into two types. Firstly, it is aimed to access the computer data by stealing the administrator rights. Secondly, it is aimed to take down the target computer.

II. TYPES OF CYBER ATTACK

The cybercriminals to fulfill their objectives like getting access to computers, data or network uses a variety of new emerging technical techniques and some of them may overlap.

1. **Malware:** which stands for malicious software, is a general term for any software that, in the words of Microsoft, apart from how it is executed, it is a designed to cause damage to a computer, server, or a network. Trojans, viruses, and worms are types of malwares; they are different from one another based on their spread and reproduction. this attack grants

root access to the attacker, by this attacker can take remote control of a system and may disable the machine or network.

2. **Phishing:** Through this technique, the hacker sends fraudulent emails or communications most like as a reputable source to a target victim to take some hazardous action. the receiver is trapped to enter confidential information like bank transaction OTPs, telephone number, username and passwords by leading them into phony website or tricked to click a link that leads to download malware by disguising as important document. some phishing emails are in particular written for treasured target people in an attempt to influence them to offer beneficial information, but many are as an alternative basic and sent to heaps of potential victims.

3. **Ransomware**: Ransomware encrypts a victim's files and is a type of malware. Here the attacker demands a ransom and promises to victim to give access to his data again after paying hundreds to thousands of dollars in cryptocurrency; the hacker also provide payment instruction to get decryption key.

4. **Denial-of-Service (DoS):** Attacks known as denial-of-service (DoS) attempts: These attempts bombard a website with fictitious requests in an effort to force it to respond to them, preventing legitimate users from accessing it. By preventing civilians, military, security professionals, or research organizations from accessing crucial websites, this kind of attack has the potential to interfere with crucial activities and systems.

5. **Man in the Middle Attack**: It is a technique used by attackers to intercept secretly between the user and a Web Application and trying to access the conversion. For example, the attacker creates a fake login page and hacks login credentials once a user logs in and apply the same on the original one.

6. **Crypto Jacking:** In a specialized assault known as crypto jacking. Here hacker installs malware software on victim’s device or runs a Javascript code on victim’s computer browser to mine cryptocurrency. Its moto is profit and it is designed in such a way that the hacker completely hidden from the victim.

7. **SQL Injection**: It is a hacking technique; here attacker execute a malicious SQL code to access to victim’s database. A web application is designed with SQL commands to take confidential information from victims. By this hacker can add, modify and delete records from the database. This type of attack affects web applications which are using SQL databases. With this they may gain unauthorized access to sensitive data of a victim.

8. **Zero-Day Exploits**: Unpatched software attacks are referred to as zero-days. the attack got this name because of the number of days, the software developer has known about the problem. it is a software related attack; it exploits a weakness which are unaware to a developer or a vendor. A software patch means a solution to fix a zero-day attack. Zero-day attack available from white market grey and block market; they also known as legal to white range markets. The government agencies discovered that many hackers using this attack for their own hacking purpose, rather than using it for the common benefit.

III. DATA BREACH

The "Indian Computer Emergency Response Team (CERT-In)" tracked number of cyberattacks on the country and statistics reported to it, but not given entire picture of it. 13.91 million cyber security events were recorded in India in 2022, down from 14.02 million in 2021, but there were fewer reported cyberattacks. According to government statistics, 2.08 lakh events, 3.94 lakh attacks, and 11.58 lakh cybersecurity incidents were reported to CERT-In in 2018. The following list includes some of India's biggest recent cyberattacks and data breaches[1-2].

1. **Air India Data Breach Highlights Third-Party Risk:** Data breach at Air India shows third-party danger. Due to the cyberattack on the Airline Data Service Provider System (SITA), 4.5 million air Indian passengers' personal information was exposed. Airline Data Service Provider (SITA) informed to the airline about leaked data, which was collected between August 2011 and February 2021.

2. **CAT Applicants' Details Leaked to Dark Web:** Details of CAT applicants exposed to the dark web: For the "Common Admission Test 2020", which was used to choose candidates for admission to the Indian Institutes of Management (IIMs), 190,000 candidates' personally identifiable information (PII) and test results were leaked and placed on dark web or cybercrime website for sale. The hacked database contained information like names of the candidate, dates of birth, addresses, email addresses, mobile numbers, 10^{th} class grade, 12^{th} class grade, bachelor's degree information, and CAT scores.

3. **Domino's India pizza orders to dark web:** According to the CTO of cyber intelligence company Hudson Rock and Alon Gal, 180 million Domino India Pizza orders are up for sale on the cybercrime website during the year 2021 in the month of April,

4. **Trading Platform Upstox Resets Passwords After Breach Report:** In order to confirm their customer identity and also to prevent attacks and money laundering, financial service providers gathered Know-your-customer (KYC) data. On 11^{th} April 2021, "Indian trading platform Upstox" acknowledged a hack of KYC data and instructed customers to reset the passwords. It also instructed needed precautions after receiving warning email for contact details held in third-party data warehouse may be compromised; because KYC data is used for committing identity theft.

5. **Indian Patients' COVID-19 Test Results were Released Online:** The government websites leaked thousands of Indian COVID patient's lab test results. This disclosed data is about Name of patient, Test Date, Type of test, Center Name and Date of Birth of patient. the hacked URL structure indicated that, these test reports are kept on CMS platform, where all government organization use for posting Publicly Accessible Documents.

6. **Juspay User Information for Sale on the Dark Web:** In the month of January 2021, Juspay acknowledged that using an Unrecycled Access Key approximately 35 million customer accounts were hacked; it includes card fingerprints and disguised card data. It said the incident happened in August of last year. According to independent cybersecurity

expert Rajshekhar Rajaharia, the customer data is offered for sale on the dark web site for about $5000.

7. **BigB0asket User Data for Sale Online:** User information from the online grocery retailer BigBasket is being sold on the dark web, according to Atlanta-based cyber intelligence company Cyble. On November 2020, Cyble announced that a portion of a database containing the personal data of around 20 million customers was availed for sale for 3 million rupees ($40,000).

8. **Unacademy Learns Lesson about Security:** The Unacademy is a an edutech firm and it disclosed a data breach, it affected 22 million users accounts. During the May 2020, Cycle a cyber security company disclosed that list of usernames, passwords, and emails were offered for sale in the dark web.

9. **Candidate Database for Police Exams is put up for Sale:** On a database sharing forum, 500,000 Indian police personnel personal information consisting of date of birth, full name, email Id, mobile number, FIR records, criminal history, etc., was kept for sale and it was traced by CloudSEK a threat intelligent firm to a police exam conducted on 22nd December 2019.

10. **Hackers Steal Healthcare Records of Indian Citizens:** From Indian healthcare website 68 lakh patients and doctors' information was hacked by hackers and this information revealed by FireEye security firm and a US based cyber security firm on august 2019. This firm also acknowledged that this hack was carried out by Fallensky519 hacker group belongs to the country China.

11. **Local Search Provider Just-Dial Exposes Data of 10 Crore Users:** JustDial firm, a local search service provider website became a victim of cybersecurity attack on April 2019 and more than 100 million users' data containing name, gender, mobile number, date of birth, emailId and address made available for public. This information said by an independent security researcher in a Facebook post.

12. **Millions of Consumers' Account Information Exposed due to SBI Data Breach:** SBI is a largest bank in the nation, many of the security researchers stated that, SBI server is unsecured and failed to protect with a password. This attack originated from "SBIQuick", as it is a free service and it provides customers balance and recent transaction over SMS. This attack sent out around 3 million text messages to customers.

13. **Hacking of the ATM System:** In the middle of 2018, a cyberattack specifically targeted Canara Bank's ATM servers. Several bank accounts had a total of 20 lakh rupees taken out of them. There were reportedly 50 victims, and according to some reports, cybercriminals got access to the ATM card information for more than 300 people. Users of debit cards had their information stolen by hackers employing skimming hardware. The price range of transactions containing stolen data was between Rs. 10,000 and Rs. 40,000.

14. **Hacked the Aadhar UIDAI Software:** The UIDAI Aadhaar software was compromised at the start of 2018, exposing the personal data of 1.1 billion Indians who hold Aadhaar cards. According to UIDAI, 210 Indian government websites were identified to carry

online Aadhaar data about people. The majority of each cardholder's personal information, as well as Aadhaar, PAN, mobile, bank account and IFSC codes, were disclosed. Not only that, but unknown vendors were offering to sell anyone's Aadhaar information via WhatsApp for Rs. 500. You can also get Aadhaar vehicle printouts by spending an extra Rs. 300.

Scam of SIM card Swap: Two hackers from Navi Mumbai were apprehended in August 2018 after moving 4 crore rupees across several bank accounts. They took money illegally from the bank accounts of countless victims. Both attackers conducted online banking transactions using posts of false documents, stole SIM card information, disabled people's SIM cards, and blocked SIM cards. Additionally, they made an effort to hack into the accounts of other targeted businesses

IV. RECENT CYBER ATTACKS

The most prominent recent cyberattacks and what we may take out from them

1. **Capitol One:** In July 2019, the titan of internet banking Capitol One learned that its data had been hacked. Birthdates and Social Security numbers from hundreds of thousands of credit card applications were made public. The sheer scale was somewhat alarming, even though no bank account numbers were collected. As usual, Capitol One offered shameless credit monitoring to those affected and apologized profusely. But then something strange happened. The stolen information never surfaced on the dark web, and unlike the Marriott and Equifax breaches, this hack did not have the appearance of a Chinese intelligence operation. In actuality, Paige Thompson, also known as Erratic, an American, was the attacker. Because Thompson had previously worked for Amazon, she had the experience necessary to understand how Capitol One's AWS server had been seriously misconfigured, leaving it extremely exposed.

2. **Ransomware on the Weather Channel:** The Weather Channel may not seem like a necessary component of infrastructure, but for many people it is. In April 2019, when a string of tornadoes struck the American South, many viewers tuned in to The Weather Channel. On a Thursday morning, though, the channel stopped live transmission for nearly 90 minutes, which is practically unheard of in the broadcast television industry.

   It turns out that The Weather Channel had been the target of a ransomware attack. Although the attack vector has not been officially confirmed, rumors suggest that it was through a phishing attempt, one of the most frequent ways that ransomware is spread. As any TV business like The Weather Channel would be completely dependent on internet-based services to operate, the attack showed that the line between "television" and "the internet" has essentially been destroyed. It also showed how to defeat ransomware in one approach. The Weather Channel didn't pay any bitcoin; instead, they had reliable backups of the compromised servers and were able to resume operations in less than two hours.

3. **Perceptics vs. U.S. Customs and Border Protection:** Sadly, the pattern was rather common: a hacker gains access to a company's servers, steals valuable information, and then demands a ransom. When the executives don't pay up, the information starts to appear on the dark web for sale, where its significance is realized to a greater extent.

Data that was stolen from the U.S. Customs and Border Protection agency (CBP) turned out to be extremely significant; no one was unaware of the irony that the organization responsible for guarding the nation's borders was unable to protect its own data. Perceptics, a contractor that provides all the license plate scanners for the border agency as well as to a variety of other U.S. and Canadian government departments, was in reality largely to fault. Perceptics was then hacked, and the material was made public by the attacker "Boris Bullet-Dodger" when ransom negotiations with executives failed. The stolen pictures of automobiles and drivers had actually been downloaded from CBP's computers to Perceptics' own servers, in violation of government policy.

The situation raised concerns about how the government and contractors interact as well as the propriety of authorizing the collecting of biometric information. The government first decided to stop doing business with Perceptics after the incident, but finally decided to resume it.

4. **Citrix Violation:** Everyone should be concerned when a company gets breached that is also in the cybersecurity industry, but it also serves as a warning that even security suppliers sometimes struggle to instill a security culture within their own organizations.

   Consider Citrix as an example. The business produces VPNs that encrypt millions of internet connections and works closely with the American government. But in March 2019, it was still the target of a "password spraying" assault, which is essentially when a hacker uses a large number of quick login attempts using passwords that are easy to remember and commonly used (such "password123" and similar). The attack most likely originated from a group connected to the Iranian government. Thankfully, the attackers were unable to penetrate Citrix's systems too far, although the business did commit to overhaul its internal security culture.

5. **Ransomware Attacks in Texas:** In August 2019, ransomware crippled the computer systems in 22 small Texas communities, preventing their governments from offering essential services like issuing birth or death certificates. How did one hacker use the REvil/Sodinokibi ransomware to assault such a wide variety of towns? An IT vendor who offered services to all of these municipalities, all of which were too tiny to sustain a full-time IT staff, was the only weak link.

   If that kind of group behavior revealed a vulnerability, there was also a strength in cooperation. The communities joined together with the Department of Information Resources of the Texas state government rather than caving and paying the $2.5 million ransom requested. In contrast to areas like Baltimore, where systems were out for months, the agency oversaw a remediation operation that put the cities back on their feet in a matter of weeks.

6. **WannaCry:** In May 2017, the ransomware attack known as WannaCry spread quickly. It took control of afflicted machines, encrypted the data on their hard drives, and then demanded payment in Bitcoin to unlock them. This is typical of all ransomware. Particularly in systems at NHS-run hospitals in the UK, the malware became entrenched.

   However, malware is nothing new. The method employed by WannaCry to spread was what made it noteworthy and frightening: it used code that had been covertly

produced by the US National Security Agency to exploit a flaw in Microsoft Windows. The exploit, known as EternalBlue, had been taken and leaked by a hacker collective known as the Shadow Brokers. Although Microsoft had already corrected the issue a few weeks prior, many systems weren't updated. Microsoft was incensed that the US government had developed a weapon to take advantage of the vulnerability rather than alerting the infosec community.

7. **NotPetya:** When Petya first appeared in phishing emails in 2016, it was merely another type of ransomware. Its key feature was that it encrypted the master boot record of infected PCs, making it nearly impossible for victims to access their contents.

   Then, suddenly, in June 2017, a much more dangerous variant of the malware began to spread. It was distinct enough from the original that it was given the name NotPetya; its initial method of distribution used hacked Ukrainian accounting software, which it disseminated using the same EternalBlue exploit as WannaCry. Although Russia denies it, NotPetya is largely thought to have been a cyberattack by Russia against Ukraine, perhaps ushering in a new era in which governments use weaponized malware.

8. **Ethereum:** Even while it may not have had the same level of notoriety as some of the other items on our list, the amount of money involved in this one justifies its inclusion. A cryptocurrency similar to Bitcoin called Ether was stolen in July from the Ethereum software platform for $7.4 million in a matter of minutes. Then, a $32 million heist occurred a few short weeks later. Concerns regarding the security of blockchain-based currency were raised by the entire episode.

9. **Equifax:** In July 2017, the enormous credit rating agency revealed that "criminals exploited a U.S. website application vulnerability to gain access to certain files," obtaining personal data for close to 150 million people. The aftermath that followed infuriated people even more, especially when it appeared that the website Equifax set up for consumers to check if their information had been exposed was mostly intended to market services.

   The Equifax hack is particularly terrible, according to Ed Szofer, CEO of SenecaGlobal, "because they had already been told about the fix — it needed to be implemented in a tool called Apache Struts that they use — well before the breach even happened." However, they did not do it in a timely manner. This was not a technological issue because the technical answer was already known; rather, it required a change in culture and resources to prevent such breaches from occurring. Equifax possessed the necessary resources, but it was obvious that the company lacked the proper culture to guarantee that the proper procedures were in place and adhered to.

10. **Yahoo:** Honorable mention goes to this significant hack of Yahoo's email system, which took place back in 2013. However, it wasn't until October 2017 that the full extent of the attack, which affected all 3 billion Yahoo email addresses, was revealed. Passwords and backup email addresses that were encrypted using antiquated, simple-to-crack methods were among the stolen data, which attackers may exploit to break into other accounts. In addition to the impact on the account holders, the breach may prompt a review of Verizon's acquisition of Yahoo, even though that transaction has already been completed.

The most terrifying aspect of this breach is that there are likely more like it out there due to the culture of secrecy that kept it hidden. For obvious PR reasons, nobody wants to share a breach, according to Mitch Lieberman, director of research at G2 Crowd. However, the reality finally surfaces. What more are we unaware of?

11. **GitHub:** 1.35 TB of traffic per second was directed at the well-known website on February 28, 2018, when a significant denial of service attack targeted the version control hosting provider GitHub. The attack's sheer size was concerning; it outperformed the massive attack on Dyn in late 2016 that peaked at 1.2 TB per second, even though GitHub was only temporarily taken offline and was able to completely defeat it in less than 20 minutes.

    Even more concerning was the attack's support system. The GitHub attack took use of servers using the Memcached memory caching technology, which can return very large chunks of data in response to simple requests, unlike the Dyn attack, which was the result of the Mirai botnet, which required software to infect thousands of IoT devices.

    Memcached generally provides little in the way of security to stop malicious attackers from faking IP addresses and blasting massive volumes of data at unaware victims. Memcached is intended to be used only on protected servers running on internal networks. Unfortunately, there are thousands of Memcached servers available on the internet, and DDoS attacks are increasingly using them. It is not fair to say that the servers have been "hijacked" because they would happily transfer packets wherever they are instructed without posing any queries. Days after the GitHub attack, a second DDoS attack using Memecached blasted an undisclosed U.S. service provider with 1.7 TB of data per second.

V. PENETRATION TESTING TOOLS

While some of the tools we've covered here are essentially Swiss Army knives that may assist you in doing various types of pen testing, others are more specialized. We'll examine the categories in which our chosen tools fit and also highlight some of the top penetration tools that are currently accessible for download[8].

1. **Tools for Network Penetration Testing:** A pen tester needs tools that can assist them access the network architecture of their targets because the stereotypical hacker spends their days breaking into networks where they have no business being. This group includes all of our top recommendations, including “Kali Linux, nmap, Metasploit, Wireshark, John the Ripper, and Burp Suite”. The packet manipulation programme ‘Scapy’, the attack and audit framework ‘w3af’, the vulnerability scanners ‘Nessus’, ‘Netsparker, and Acunetix’, are some more well-liked network pen testing tools.
2. **Web Application Penetration Testing Tools:** tools for checking the security of web applications. A pen tester should put a lot of effort into web-facing applications because they are one of the key attack surfaces that every organisation has to safeguard. This will allow them to thoroughly evaluate their target's security. “Nmap, Metasploit, Wireshark, Jon the Ripper, Burp Suite, ZAP, sqlmap, w3af, Nessus, Netsparker, and Acunetix can all help with this task, as can ‘BeEF’, a tool that focuses on web browsers; web application vulnerability scanners ‘Wapiti’, ‘Arachni, Vega, and Ratproxy; diresearch’, a command-

line tool designed to brute force directories and files on ‘webservers; and Sn1per’, a “all in one" pen testing framework”.

3. **Database Penetration Testing Tools:** software for assessing database security. It's crucial for a pen tester to have the tools necessary to pick locks if a hacker's objective is to exfiltrate valuable data, which is usually hiding in a database somewhere. ‘Nmap and sqlmap are crucial resources for this. The same goes for BSQL Hacker, an automated SQL injection tool, and SQL Recon, an active and passive scanner that explicitly targets and attempts to identify every Microsoft SQL Server on a network’.

4. **Automated Penetration Testing Tools:** By hand, it might take years to identify every potential vulnerability in a given system. To expedite the process, several pen testing solutions provide automated features. In this aspect, “Metasploit, John the Ripper, Hydra, Sn1per, and BSQL Hacker stand out”.

5. **Open-Source Penetration Testing Tools.** Pen testing has its origins in the hacking community, which has a strong commitment to the open-source movement. Other than Burp Suite, all of our top recommendations for tools are open source, including “Scapy, BeEF, w3af, Wapiti, Arachni, Vega, Ratproxy, and Sn1per”.

VI. SECURITY TOOLS

The CERT-IN promote few cyber security tools, which are used to remove cyberattacks and botnet from windows operating system and android operating system. They are explained as following [10-16]

1. **Free Bot Removal Software for Windows:** eScan Antivirus, K7 Security, Quick Heal

2. **Free Bot Removal Tool for Android:** eScan Antivirus.

3. **Free Mobile Security Application for Android:** eScan Antivirus, C-DAC Hyderabad

4. **Other Relevant tools**

- **USB Pratirodh:** This software program is a Desktop Security Solution that manages the use of portable storage devices alike USB Flash Drives, External Hard Drives, Mobile Phones, and some other supported USB Portable Storage Devices.
- **AppSamvid:** This tool is a desktop-based application whitelisting solution for Windows called AppSamvid; it is permitted to execute only pre-approved list of executable files.
- **Browser JSGuard:** This utility is a browser plugin; it uses heuristics to identify and protect against malicious HTML and JavaScript assaults sent through the web browser. When accessing any harmful websites, it warns the user and gives an in-depth examination and risk report of the website.

VII. SECURITY MEASURES TO PREVENT CYBER ATTACKS

1. Provide employees with security awareness training to inform them of new cyber-attacks.
2. Keep all programs and systems regularly patched with the most recent security updates.
3. Use email authentication methods like DMARC, DKIM, and SPF to protect your email domain from cyberattacks based on email [5-7].
4. Conduct routine vulnerability assessments and penetration tests to identify and fix any existing network and online application vulnerabilities.
5. Limiting employee access to private or delicate information as well as their power to install software.
6. Use extremely secure passwords for your accounts, and make sure to update them frequently [11].
7. Steer clear of the open password sharing practice at work.

VIII. CONCLUSION

India had around 851 million internet connections as of the end of the fiscal year 2023. despite the fact that around 70% of Indians reside in rural areas, metropolitan areas still have more connections than those in rural areas. Urban areas had 507 million internet connections as of 2023.

Data breaches can immediately affect several hundred million or possibly billions of individuals in a modern data-driven age. Data breaches have grown in scale along with the digital transition because attackers have exploited our everyday dependence on data. Although the size of cyberattacks in the future is impossible to foresee, this list of the biggest data breaches from the twenty-first century demonstrates that they have already grown to be very large.

REFERENCES

[1] Soumik Ghosh, The biggest data breaches in India, https://www.csoonline.com/article/569325/the-biggest-data-breaches-in-india.html, 2022
[2] Soumik Ghosh, The 15 biggest data breaches of the 21st century https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, 2022
[3] https://www.statista.com/statistics/1196721/india-internet-connections-in-rural-and-urban-areas/ India: number of internet connections in rural and urban areas 2023, https://www.statista.com/statistics/1196721/india-internet-connections-in-rural-and-urban-areas/, 2023
[4] Cyber Jagrukta Divas | Cyber Jagrookta Diwas, https://kratikal.com/cyber-jagrukta-divas, 2022
[5] DMARC, https://threatcop.com/blog/what-is-dmarc/, 2021
[6] DomainKeys Identified Mail (DKIM), https://threatcop.com/blog/dkim, 2021
[7] Sender Policy Framework (SPF): https://threatcop.com/blog/spf-authentication, 2021
[8] VAPT Services | Penetration Testing https://kratikal.com/vapt-services, 2022.
[9] Password Safe from Hackers, https://threatcop.com/blog/how-to-keep-your-password-safe-from-hackers/, 2023
[10] Security Tools, https://www.csk.gov.in/security-tools.html, 2023
[11] M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji, Cloud Computing : Research Issues and Implications International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.2, April 2013, pp. 133~139 ISSN: 2089-3337
[12] B Vishnuvardhanand B Manjula, R Lakshman Naik, Pre-Authorization And Post-Authorization Techniques For Detecting And Preventing The Session Hijacking, International Journal of Future Generation Communication and Networking, Volume:14, Issue:1, Pages:359-371, 2021

[13] Dr.V.Bapuji,Dr.P.Venkateshwarlu, Jogugla Ajay, "Detection and Attribution Of Cyber Attacks In IoT Enabled Cyber-Physical Systems",Juni Khyat (UGC Care Group I Listed Journal),ISSN: 2278-4632,Vol-13, Issue-08,http://junikhyatjournal.in/no_1_Online_23/29_online_aug.pdf, August 2023

[14] de Bruijn, H. and Janssen, M. (2017) 'Building Cybersecurity Awareness: The need for evidence-based framing strategies', Government Information Quarterly. doi: 10.1016/j.giq.2017.02.007

[15] Fink, G. A. et al. (2009) 'Visualizing cyber security: Usable workspaces', in 6th International Workshop on Visualization for Cyber Security 2009, VizSec 2009 - Proceedings. doi: 10.1109/VIZSEC.2009.5375542.

[16] Hámornik, B. P. and Krasznay, C. (2018) 'A team-level perspective of human factors in cyber security: Security operations centers', Advances in Intelligent Systems and Computing, 593, pp. 224–236. doi: 10.1007/978-3-319-60585-2_21

