ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering [e-ISSN: 2067-3809]
TOME XIII [2020] | FASCICULE 3 [July – September]

[1.]Sakshi SINGH, [2.]Suresh KUMAR

THE TIMES OF CYBER ATTACKS

[1,2.]Department of Computer Science Engineering, AIACTR, Delhi, INDIA

Abstract: Cyber security's importance is on the rise. Our world relies on technologies more than ever before. Government, military, organizations, financial institutions, universities and other businesses collect, process and store a large amount of information on computers. This trend is growing faster every day. As computers become a major source of information, they need to be protected. Every day a new type of cyber-attack came into an act which makes digital data more vulnerable day by day. Cyber security is the practice of ensuring the integrity, confidentiality, and availability (ICA) of information. It requires a broad variety of resources to secure networks, computers, services and data against threats or non-authorized entry, which encompasses best practices for risk control techniques and technologies. In this paper, we will address generations of cyber-attacks, attacker strategy, and biggest cyber -attacks in India. The statistical data of cyber-attacks and security will be discussed. The paper will also clarify emerging concepts of information technology and potential protection developments. In this article, intelligent protection strategies will be clarified to secure information from multiple intruders.

Keywords: confidential data, cyber-attacks, cybercrimes, cyber security, defense, hackers

INTRODUCTION

Cyber protection requires technologies, processes and acts to prevent interference, intrusion or unwanted access to networks, equipment, facilities and documents. This involves data storage. It may also be considered protection in the area of information technology. It is important, as states, businesses, and financial institutions and medical organizations gather, process and store data on computers and other tools without precedent. Sensitive details, be it intellectual possession, financial records, personal information or some other records category that could have adverse impacts on unwanted entry or disclosure, may be a major part of this database.

The corporation that transmits sensitive data through networks and other instruments in the market sense determines the discipline of information management, and the processes that are used to administer and retain it.

As cyber threats are increasing in scale and scope, businesses and institutions, in particular those responsible for safeguarding public protection, health and financial data, have to take action to secure their confidential details for company and workers. Cybercrime is one of the world's largest and one of the biggest risks to any organization.

The impact on society is reflected in the numbers. Cyber protection firms estimate the worldwide expense of cybercrime to $6 trillion by 2021 []. This reflects the largest global capital transition in history, threatens opportunities for creativity and production and would be more lucrative than the entire international trade in all big illegal substances.

The cost estimates of damage are based on historical statistics of cybercrime including recent year-over-year growth, a dramatic rise in the hostile nation-state and gangs-hacking activities, and a greater cyber-attack surface by 2021. Cybercrimes involve harm, devastation, burglary, stealing of profitability, intellectual property, burglary of personal and financial data, embezzlement, fraud, normal-term post-attack intrusion, forensic analysis, repair and erase hacked and reputational abuse.

India, with over 560 million internet users, ranks just behind China, is the second largest online platform in the world. According to Internet and Mobile Association of India (IAMAI) [1,2], more than 600 million internet users are projected in India by 2021. In 2015 just 17% of Indians were able to use the internet. There were 483 million internet users in India in 2018. In 2023, 666.4 million internet users will be registered, according to the study [3]. It will lift the figure. Because of its untapped potential, India is the world's second largest online sector. The bulk of internet users in India are cell phones internet users who allow the most practical alternatives to the costly hardware that desktops and networks require. As of 2016, India's mobile Internet usage figures is 320.57 million and Indian Internet users estimated 492.68 million by 2022. 390.9 million users were able to navigate the internet via cell phone in 2018. The number will hit 500.9 million internet users in 2023 [3]. This amount is anticipated.

The paper is structured as follows: Section II covers the annual statistical data about cyber-attacks and the expenses spent on them. Section III defines various cyber-attack generations with examples over the last few decades. Section IV explains the biggest cyber-attacks that took place in India. Section V explains how cybercrimes flourish in future and estimated investment on them. Section VI describes how future technologies should be developed with inbuilt security. Section VII suggests some smart security solutions that will help to tackle future cybercrimes and economic losses done by them to the nation. Section VIII describes the conclusion.

LITERATURE REVIEW

Any significant violation of information security will collapse and destroy the credibility of an entire organization. Cybersecurity risks are not just a problem of major corporations, such as banks, software firms, and state departments, but also the obligation of any other citizen involved with their records. The rate of cyber-crimes is increasing day by day and therefore the analysis of information security statistics and patterns in past years is necessary for us to understand the diabolistic and illegal forms in which data abuses arise and take steps to be secured.

» 2017

For cybercrimes, 2017 was a high year. The number of cyber-safe accidents has almost doubled from 2016 according to the Online Confidence Alliance [4]. This huge spike, from approximately 82,000 accidents in 2016 to approximately 160,000 in 2017, has been credited in the "2017 Cyber Report" [5]. The eye-catching figures of cybercrime in 2017 were further helped by high-profile ransomware attacks like WannaCry and NotPetya. The estimated expense of a violation was $3,62 million in 2017, according to the Ponemon Institute and IBM's 2017 "Expense of Data Breaching Report" [6].

The most troubling evidence cited in this study were that, with the implementation of public management practices such as patching apps and performing phishing instruction, 93% of accidents may have been stopped. Although 52% of infringements culminated in "real hacking," 15% were induced by lack of safety devices, 11% were triggered by inadequate internal danger control and 8% by phishing, respectively [5].

» 2018

The biggest DDoS attack ever reported was endured by GitHub [7] in 2018. The assault culminated in 1.3 terabits of GitHub traffic for a second. A team of security experts from Security Research Labs took to the Hack in the Box security conference to reveal their project: two years in the reverse engineering phase of the operating systems of Android phones, which showed that some handset makers withhold security fixes from users.

With fines of up to 20 million [8] or up to 4% of the annual worldwide turnover for those companies caught mishandling user data, GDPR promised to usher in a new age for the processing of personal data.

» 2019

In 2019, the cyber technology industry grew by 8.7% and the money invested on data management, rules and data privacy law enforcement tools was $124 billion (Weekly computer) [9,10]. Around 94% of targeted emails use the payload or malware root to add harmful data. 91% of cyber-attacks start with a "spear-phishing" text, an increasingly popular type of phishing that allows more precise and personal use of knowledge regarding a target (Be4Know) [11]. Billions of dollars of damage is triggered by cybercrimes, as per analysis by Juniper, the figure reached $2 trillion by 2019 [12].

CYBER-ATTACK GENERATIONS

# The Ist Generation: In the late 1980s, hackers mounted virus attacks on standalone PCs, typically propagated via disks. The affected private users and companies contributed to the creation of anti-virus (AV) products focused on signature info. Examples of first-generation assaults are:

» Elk Cloner (1982): the first computer virus in the world.

» Brain (1986): booting attack.

# The IInd Generation: In the mid-1990s, quickly expanding worm attacks emerged straight from the omnipresent Internet, which forced businesses to build a firewall at the infrastructure's periphery to keep the bad people out. Examples of IInd generation attacks include:

» The Morris Worm (1988): One of the first computer worms, leading to the US first felony conviction under the Computer Fraud and Abuse Act.

» Melissa (1999): A mass mailing macro virus.

# The IIIrd Generation: During the first years of the new century, criminals began exploiting bugs during software that could impact the businesses exploiting them. That is also about the period when the purpose of the offender switches from appreciation to remuneration. Initially, the botnet was used, particularly for the spam distribution. This attack generation contributes to the creation of IDS systems, which soon incorporated correction capability and became Intrusion prevention systems. Signatures were already based on IDS / IPS. Examples of assaults from the third century include:

» ILOVEYOU (2000): A worm infecting tens of millions of Windows machines.

» SQL Slammer (2003): Denial of service on 75,000 hosts.

# The IV Generation: During the early part of the last decade, there were no signs of the emergence in targeted attacks. During a conversation on the absence of clear evidence regarding weapons of mass destruction, citizens were prompted to follow the word "hidden unknowns" invented by then American defence secretary Donald Rumsfeld. Malware application consistency increases and the

first rootkit starts to pop up. Types of threats from the fourth generation include:

» Stuxnet (2005-10): State-sponsored development, targeting SCADA systems in critical infrastructure, including the Iranian nuclear program.

» The Target Breach (2013): Not a virus or worm, but a targeted attack on the clothing retailer. The details of 40- 70 million credit cards stolen, 110 million people's personal information breached.

» The DYN Attack (2016): Not a virus or worm, but a massive distributed denial of service (DDOS) attack on the major DNS provider.

# The Vth Generation: A wide-ranging mega-attacks funded by the government began in 2017 so that several businesses may execute them. Cybercrime has its internet and escrow networks. There's a busy null-day market. Examples of assaults from the Vth wave are:

» WannaCry (2017): Major ransomware attack affecting 200,000 computers across 150 countries.

» Petya and NotPetya (2016-17): Variance of ransomware used against machines across Europe.

BIGGEST CYBER-ATTACKS IN INDIA

≡ SIM Swap Fraud

In August 2018, Navi Mumbai arrested two men for cybercrime. They participated in fraudulent practices with regard to the money transfer from the accounts of a variety of people, unlawfully collecting details on the SIM card. This fraudsters obtained details from citizens and prevented the usage of false documents on their SIM cards. They had to transfer four Indian Rupees out of different accounts successfully. We also went to access a few corporations' profiles [13].

≡ Cyber Attack on Cosmos Bank

The Cosmos Bank's Pune branch was targeted in August 2018 by a brazen cyber assault, which saw the loss of almost 94 Crores rupees. By breaching the Cosmos Bank's computer, In Hong Kong, Hackers cleaned out and passed the funds to a trust. The lawsuit was put before Cosmos Bank with a Pune court of cyber assault.

Hackers hacked into the bank's ATM network and stole many details from owners of visas and debit cards. The assault did not go against the cohesive banking solution of Cosmos Bank. The deposits and balance sheets remain unchanged and have little impact on the financial statements of the owner. The switching process was built to function as the node of communication between the payment portals and the bank's central banking solution.

The malware assault on the switching network created many false alerts that verified many external demands for visas and debit cards. In 28 nations, there were 14,000 sales, more than 450 tickets. 400 cards and 2,800 transactions were used at the state level. This was the first malware assault to break up the link between the payment gateway and the Indian bank [13].

≡ ATM System Hacked in Kolkata

Fraudsters pirated in July 2018 and wiped off almost 20 lakh rupees of different banks' accounts on ATM servers at Canara Branch. More than 50 people were killed and over 300 ATM customers were accused of providing account data in India.

Hackers used skimming machine on ATMs to capture debit cardholders' data to execute a minimum purchase of INR 10,000 and an INR cap of 40,000. Two people who collaborated for a foreign group used skimming operations to collect bank data were arrested on 5 August 2018 in New Delhi [13].

≡ Websites Hacked

Between April 2017 and January 2018, more than 22,000 websites have been compromised. The Indian Cyber Emergency Response Team's figures indicate that over 493 pages, including 114 government-owned websites, were compromised with malware spreads.

The attacks were to gather information about users on the network infrastructure and device data [13].

FUTURE OF CYBER-ATTACKS

The cybercrime industry has risen with the economic growth of at least $1.5 trillion annually. It is projected to hit $300 billion by 2024 for the cyber-security sector.

In 2021, it is estimated that 70% of all purchases for crypto-currencies would be for illicit activity. Cyber-crime costs are estimated at 6 trillion dollars globally by 2021 for corporations and organizations. The loss reported being 20 billion dollars in Ransomware worldwide. An organization's total cybercriminal loss is projected to be 13 million dollars annually [14,15]. In the near-decade, there are a variety of big cyber threats.

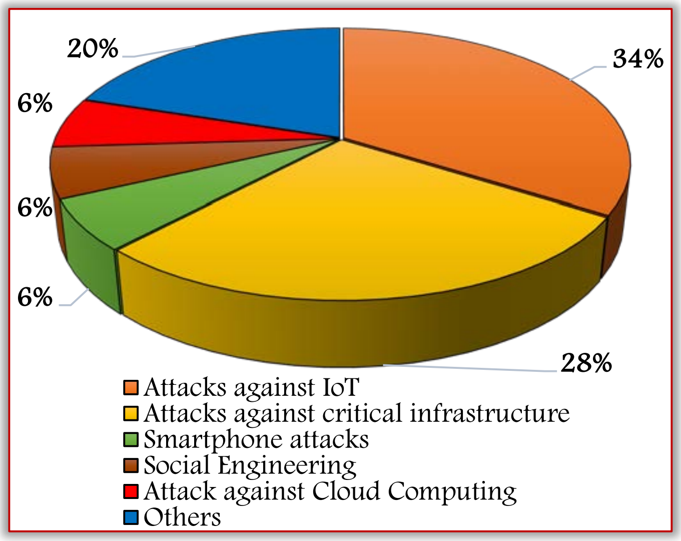

Figure 1. Major cyber-attacks by 2025

Attacks against IoT would be 34%. A maximum of 98% of IoT computer traffic is authenticated, exposing network data that is sensitive and private. 28% of sensitive infrastructure threats and 20% of devices would be targeted [14]. Using a smartphone and other media, attackers attempted to pass on confidential details to citizens. Such assaults are recognized as virtual infrastructure and will carry 6% of assaults in the future.

There are also ongoing advances in cloud infrastructure, which have several bugs that cyber attackers or malicious insiders may use.

DESIGNING FUTURE TECHNOLOGY WITH SECURITY

The design of future technologies must provide security. Adding protection afterwards is not enough or viable anymore. Innovation in defence will have more efficient and insightful approaches to face threats. For cooperation and advancement of adoptions, networks and safety requirements must be available. Throughout the design and implementation of their goods, security and protection suppliers must be assured. To avoid compromise and render safety clear to the user, goods and services must be solid. For both parties and systems in the digital world, encryption needs to secure data while it is accessible or used.

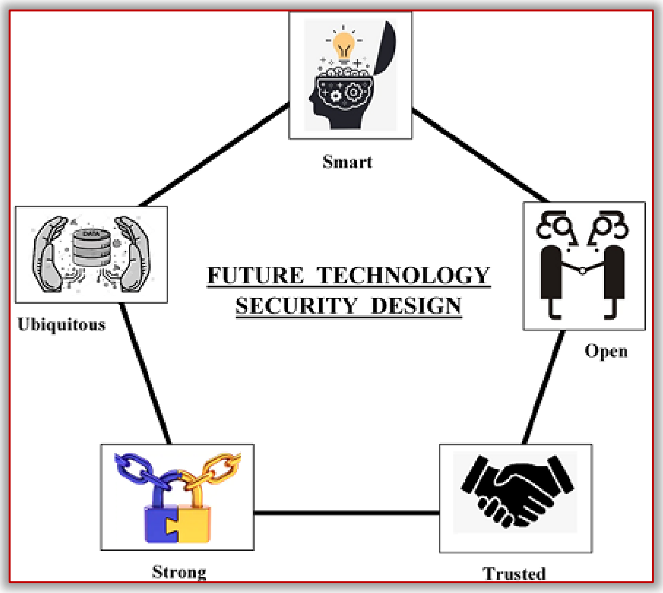

Figure 2. Future Technology security design

SMART SECURITY SOLUTIONS

Today, all our critical systems are interconnected and computer-driven. The digital and Internet of Things (IoT), Artificial Intelligence (AI) and Big Data and cloud storage etc. would be more relevant to day-to-day tasks and decisions. Such tools have a significant impact on their degree of weakness, relations and complexities.

In the future, cyber-attack based technology for Protection and Offensive can be built by organizations. The cybercriminals and hacktivists will try to utilize cyber-technology to transmit their message and raise revenue and violence in the tribunal.

To order to contend with cyber threats and to secure records, particular information defence platforms and technology would need to be more mature and more complex. Defence systems need to be linked in such a way that they may function in real-time. Human will not be able to handle all information attacks so in future the dependency on AI will increase. Also, there is a need to cultivate next generation and advanced cyber experts who will know how to drive and develop those systems. We need a stronger protection approach to secure our infrastructure, technologies and knowledge.

For now, hacking has become the number one cause of the intrusion, accompanied by ransomware, intruder and outsider agents and unintentional violations. The number of attacks which lead to device failure and data loss continues to grow. Tougher privacy and other legislation related to cybercrime will be implemented to determine and prosecute criminals and avoid cyber-attacks.

This is claimed that what hackers and criminals would be seeking would decide the future of information protection. And it will mostly be the health-related information and also the wealth like credit card and other financial information. For these regions, data defence should then be stronger because the information is the most valuable commodity.

The security departments have traditionally been focused on on-site applications but now Azure, cloud with AWS, and SaaS software can be included, causing other critical details to be compromised or breached. Capable computer frameworks must be implemented that can track, identify and handle cyber-attacks and deter them in real-time.

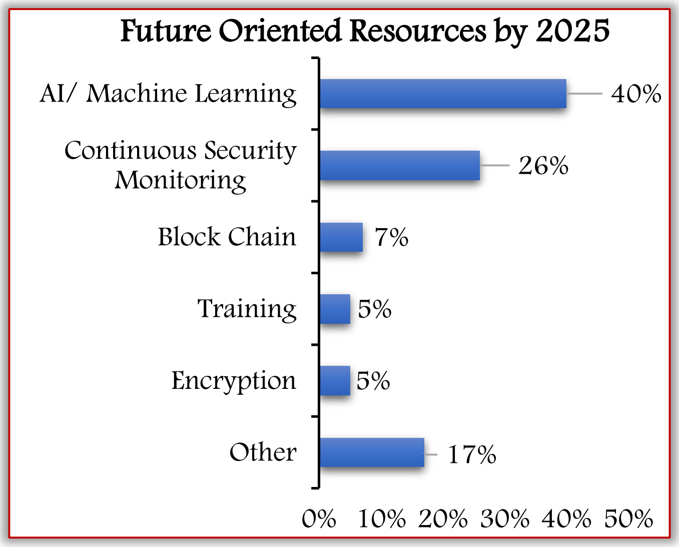

Figure 3. Resources that are used for security purpose in future [14]

CONCLUSION

The defense of our classified documents, personally identifying details (PIIs), secure health records (PHIs), financial knowledge, intellectual property, technology and computer networks against intrusion and undermining attempts by offenders and opponents is an essential part in cybersecurity.

Cyber threats from every organization's level can arrive. It was becoming really important to warn people about social manipulation schemes like phishing and more sophisticated computer security threats, such as ransomware (such as WannaCry, NotPetya). In this article, we have discussed the drastic increase in the number of internet users in the last few years with the biggest cyber-attacks that took place in India.

The generations of various cyber-attacks give us a clear view of how cyber-attacks technologies upgraded from the very beginning. We have also discussed how cyber-attacks will affect us economically in the upcoming future and counter technologies to overcome all those cyber-attacks. Smart security solutions are suggested to tackle them.

References

[1] Indian Internet 2019, https://cms.iamai.in/Content/ResearchPapers/d3654bcc-002f-4fc7-ab39-e1fbeb00005d.pdf
[2] https://economictimes.indiatimes.com/tech/internet/india-has-second-highest-number-of-internet-users-after-china-report/articleshow/71311705.cms?from=mdr
[3] Cyber Security, https://niti.gov.in/sites/default/files/201907/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
[4] https://www.internetsociety.org/news/press-releases/2019/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-45b-in-2018/
[5] 2017 Cybercrime Report, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
[6] 2017 Cost of Data Breach Study, https://www.ibm.com/downloads/cas/ZYKLN2E3
[7] https://www.wired.com/story/github-ddos-memcached/
[8] https://privacy.net/cybersecurity-statistics/
[9] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
[10] https://www.computerweekly.com/
[11] https://www.knowbe4.com/
[12] https://www.juniperresearch.com/document-library/white-papers/the-future-of-cybercrime-white-paper
[13] https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/
[14] https://www.radarservices.com/resources/study2025/
[15] CYBERSECURITY FUTURES 2025 INSIGHTS AND FINDINGS, https://cltc.berkeley.edu/wp-content/uploads/2019/02/Cybersecurity-Futures-2025-Insights-and-Findings.pdf

ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering
ISSN: 2067-3809
copyright © University POLITEHNICA Timisoara,
Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://acta.fih.upt.ro