Beyond Everything: The Role and Importance of Cybersecurity in Smart Era

Shamila Mohammed[1], Roshni Nawaz[2], Amit Kumar Tyagi[3]

[1]Department of Computer Science & Engineering, Malla Reddy Engineering College, Hyderabad,India

[2, 3]School of Computing Science and Engineering, Vellore Institute of Technology, Chennai Campus, Chennai, 600127, Tamilnadu, India

[1]shamila.m@gmail.com, [2]roshninawaz26@gmail.com, [3]amitkrtyagi025@gmail.com

Abstract. In a world where everything is ruled by technology and software, it is very important that our personal and private files and details remain secure and undiscovered by other systems in the network. Today, the immediate way of sending any urgent information is through e-mails, WhatsApp etc., all of which is sent and travels through the network (public or private). A network is an interconnection of billions of computers, these computers are connected to each other. Though they cannot be accessed directly due to restrictions and different protocols and nature of different systems, but it is not impossible. There have been many major (serious) cyber-attacks in the past three decades. Even today situation is that developed counties are interested to do launch trade war or cyber war against their enemy nation except a physical war (without killing anyone, demolishing a nation financially). Note that many computer criminals are wanted till date. Now days, everything from money transaction, sending or sharing important/ confidential information and even in hospitals medical equipment like in an oxygen cylinder the pressure and speed of the devices are all monitored by machines that are operated on software. So, any unauthorized access into any software with criminal intention not only affects property but also tampers with health of people (or patient or citizen of a nation). So, to detect any kind of intrusion into a software or system, many researchers recommend to use Intrusion Detection Systems (IDS), but still unable to secure systems completely. Hence, this research article provides the essential information like importance of keeping user's information private and secure, algorithms that can protect the system from intrusion, vulnerabilities in network and the major cyber-attacks in history (in previous decade) and how to prevent yourself from such kind of attacks and to be aware (with providing several rules, policies, digital forensics, threat hunting, etc.) in this smart era.

Keywords- Ethical Hacking, Cybersecurity, Intrusion Detection System, Cyber-Crime, Digital Forensics**.**

1. Introduction about Cybersecurity

Today big issue is that "How everything is connected". We can see that in many applications are connected to smart devices and running properly and generating Big Data (on cloud or its edge) [1]. For example, at home a computer system is directly linked to the internet through a modem or a phone line cable. Similarly, in a company of a university each computer's Network Interface Card (NIC) is linked to the LAN(Local Area Network) inside that particular area. Internet Service Provider (ISP) is linked to larger ISP's and they are linked to largest ISP's. These ISP's act as "backbones" of a country or region and they are connected through fiber optical lines, undersea cables and satellite links. It is a network of network, called internet, through which peopleshare information with each other via wired/ wireless mode. But, there are people in the world with good and bad intentions; people with bad intention only look for their benefit in everything without thinking about the consequences others have to face. There are people who have the skills of breaking into the network to find potential threats and weak points that malicious hackers can use to exploit, i.e., can exploit some other people' s network for their financial use, for example, Botnet [2], Virus, malware, Trojan Horse, etc. These are the few example which affect citizens, also to nation (in terms of development and growth). In 2016, we have seen many cyber-attacks, also cyber-attacks on nuclear sites to pull down many countries. Today's government do not require a physical war, they can won war without a bullet, i.e., via attacking on the public network of a nation. Also, implementing many restrictions on trade, technology, etc., a nation's development can be pulled down.

Cybersecurity and Ethical Hacking

Smart devices collectively played a major role in the lives we live in the 21st century. In today's technology-driven world, engineering is the cornerstone and driver of innovation of the devices we utilize daily to improve our quality of life. These smart devices are connected through internet, create a internet enabled architecture. Cyber infrastructure is a technological and sociological solution to the problem of efficiently connecting laboratories, data, computers, and people with the goal of enabling derivation of novel scientific theories and knowledge. Note that since the data packets keep circulating within the network, it is easy for hackers to insert viruses or malware into the data packets and spread it through the network.

HackingVs Ethical Hacking

Hacking is the exploitation of the extreme technical skills, a person do for their own needs, benefits and interests, called as cracker/ black hat. On another side, ethical hacking (called white hat) [3] is done by a person who is hired by companies/ organizations to break through the system (to search for potential threats and weak points in the software), through which malicious hackers (other people) can enter into companies' network or insert viruses or malware and spread through the company's network. For example, government hire some skilled people to prevent and identify lop holes in their current (using) systems, to avoid any kind of cyber-attack from the enemy's id. Black hat hacker may exploit a network for their use/ interest. For example, ransomware and Wanna Cry attack [4] (occurred in 2017), was done by some people and they infect millions of internet enabled systems word-wide and released control from the subsystem only after getting a particular amount form owner's side, i.e., this attack was completely related to ransom. Note that the person who hacks any system or software can have many motives behind them like ransom, their own selfish interests or for the benefit of the nation or mankind. There are several ways a Network/Software is Endangered/ Exploited, which are included here as:

- Open file transfer
- Insecure network
- Phishing
- Smishing
- Malware
- Malicious Apps
- Man-in middle attack
- Denial of service

Vulnerabilities on a Network (Public/ Private)

Vulnerability in a cybersecurity system is a flaw or a type of weakness that is open to attack and the confidential information stored in it is exposed to threat. A computer virus is a malicious and harmful software code that replicates itself by copying itself into another system. In simple terms, viruses is just like a program, a program is written for affecting another program (running/ implemented in another systems)software, file or document (like how a virus spreads in the body). Note that a virus is very dangerous as it can destroy a file or even collapse an entire computer system. The first virus called *creeper virus* was discovered in 1970, and the first hacker made virus came to existence in 1981 that spread through the floppy disks. The number of viruses increased a thousand-fold. Later, various attacks/ much vulnerability were measured in 19th and 20th century. By 2004, due to having a lot of awareness among citizens/ people and developed some programs for eliminating viruses completely which results in decreasing number of total attacks over the public network. But, today's we

(websites) are facing many attacks every-day. Organizations are investing a huge amount in investing/ detecting attack in systems and protection of systems against such vulnerability/ attack. Viruses are used as tools by hackers to gain unauthorized access and steal confidential information. Some types of common viruses that exist and affect the speed and performance of systems and cause corruption in files:

- Resident
- Multipartite
- Direct Action
- Browser hijacker
- Overwrite virus
- Boot sector
- Macro virus
- File infector
- Non resident
- Worms, adware, malware, ransomware , Trojan

But, today we have a big question "How to prevent or block virus in the first place" or "How to protect our businesses against malicious attacker (insider/ outsider)". Hence, this article provide a complete, we need to provide an efficient, affordable and disruptive solution, i.e., effective solution to make a cyber infrastructure attack free. Hence, the organization (remaining part) of this article is follows as: Section 2 discusses work related to secure cyber infrastructure, cybersecurity, etc., with some interesting facts. Further, our motivation behind writing this article is discussed in Section 3.Further, scope of Cybersecurity Today (in present) and Tomorrow (in future) will be discussed in detail in section 4. After this section, section 5 continues with identifying reasons behind occurring of cyber –crimes, i.e., finding Vulnerabilities in Software/ Embedded Systems. Further, available techniques and algorithms to Keep Information Safe and Secure on Web will be discussed in section 6. Section 7 discusses problems or difficulties raised during protecting businesses against many vulnerabilities/ attacks. Section 8 discusses many opportunities for Future Research Communities. Later, section 9 discusses an open discussion, which provide a detailed discussion about "Is cybersecurity really required today to us"? In last, this article (work) will be concluded with several future remarks and interesting research gaps in cybersecurity area.

1. Related Work

Any organization (either small scale or large scale) give more importance to security of their data. Each organization must identify the attack surface. As per the studies employees of the organization are responsible for 43% of the data loss. The evolution of cybersecurity has shown in figure 1.

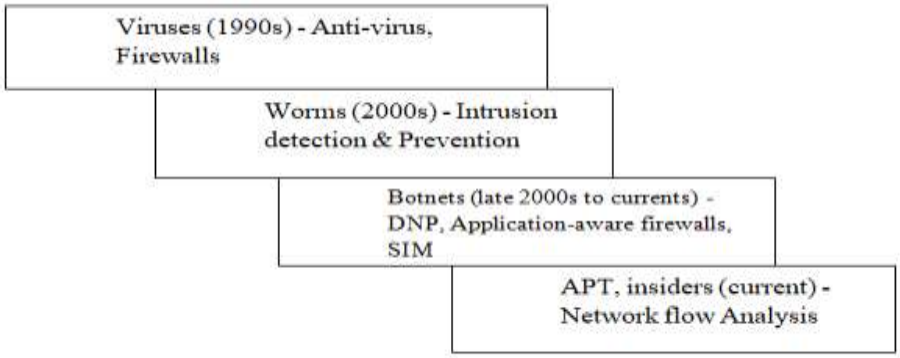

Figure 1: Evolution of Cybersecurity

Initially the organizations depend on firewalls. It can be considered as a tool or device connected to the network. It mainly monitors which all outside networks are authorized to connect or send request to their network. The organization also uses backup management as a part of disaster recovery plan. Educating employees, insisting to use strong passwords and use of security software are also some of the strategies to achieve cybersecurity. The organization must also maintain documentation on cybersecurity protocol. Table 1 represents some of the existing tools to provide cybersecurity. Cybersecurity plays a vital role in individual, families, organizations. It protect every individual from online fraud (especially it gives financial security). The number of users of internet is increasing daily. With the advancement of information technology every sector has been automated. So, it is very essential to protect the network from cybercrimes [5].

Integration of computer system with new technologies has increased the cybersecurity concern. Figure 2 gives brief introduction as state of cyber-attacks.

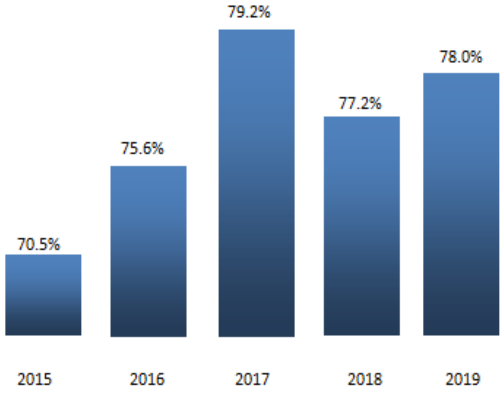

Figure 2: Frequency of attacks per year [6]

Now we will see some of the cybersecurity methods in detail. Jovanovic N et al. [7] have introduced a method to discover vulnerability in a web application program. It was implemented with the help of context /flow sensitive and inter procedural data flow analysis. This tool successfully identified 15 new vulnerabilities in three web application programs. Jan-Min Chen and Chia-LunWu [8] proposed a vulnerability scanner for detecting injection attack. Inorder to detect XSS vulnerability Michelle E Ruse and SamikBasu [9] proposed a two-phase technique which also helps to prevent XSS attack which occurs in web applications. In this, during first phase the web application code is translated to a language for which testing tools are available. In second phase, they

included monitors to capture the I/O dependencies of first phase. Gupta, M.K. et al. [10] introduced a type of software security method which can be used to develop secure software during development life cycle of software. In recent years even machine learning techniques also contributed in cybersecurity. This techniques help to differentiate whether a message is spam or not. Some of the example for machine learning techniques for spams detection includes Bayesian classifier [11], SVM [12], Map Reduce [13]. Even Artificial Intelligence (AI) and Internet of Things (IoTs) can also use for enhancing cybersecurity. AI systems can be trained to detect the smallest behaviors of ransomware and malware attacks before it enters the system and then isolate them from that system. But the main risk is that AI and ML may also exploited by attackers.

Hence, this section discusses work related to cybersecurity and its related protection or mitigation mechanisms, made by researchers in the previous decade. Now, next section will discuss our motivation behind writing article related to this important area.

2. Motivation

Today almost every possible application is implemented with smart things or work with internet enabled things. These machines share information with other devices/ machines and face many attacks now days. These attacks are DDoS attack, Phishing, Selling information to malicious or enemy users, etc. Selling information is credit card details, hospital records, accounts or passwords, i.e., when this data comes (reaches) to hand of unauthorized users. It becomes a critical issue. Together this, many vulnerabilities are also faced for online users. These vulnerabilities steal information by encrypting it and demand a ransom for its release (remove) from end user's data. For example, ransomware attack (performed in 2016) is a popular example. Note that these cyber-attacks target businesses and organizations which have important information, like hospitals and their patient records or any important information with respect to launching a new product. Such attacks need to be stopped and require a complete protection against such cyber –crimes. For providing information to general users (online users), we need to provide them a proper awareness and current implementations/ status of cybersecurity. Where is the current research on cybersecurity it is? And how attacks can be prevented before occurring on a network? This article provides complete information about cybersecurity from its evolution to till today, with covering every possible information related to cybersecurity. Hence, this section interesting scenarios with an example, and provide our motivation behind writing this article, related to cybersecurity. It shows that we require more secure methods/ algorithms in near future to protect smart infrastructure against nay attacks/ malware attack. Now, next section will discuss scope or importance of cybersecurity in present and future (in detail).

3. Scope of Cybersecurity Today and Tomorrow

Near future belongs to Artificial intelligence, Blockchain technology [14], and cybersecurity. As we see todays, Blockchain technology use is emerging in many applications every-day. Also, Fourth Industrial Revolution include Artificial Intelligence (AI) have lot of vulnerability possibilities, i.e., required attention from researchers from around the world.

As we know, increasing cyber-attacks creates more possibilities of work, i.e., creates more job opportunity for many users. Cyber-security professional is expected to protect the organization's online assets, i.e., protect information or data over public network against malicious users/ malware/ virus. It includes a file, network, firewalls, detection of vulnerabilities, also it monitor of the activities of user and hunt threat proactively. Cyber-security expert also identify the problem and provide its solution, recover from an attack, disaster recovery and backup plans, and so forth.

Today's Cybersecurity isusing by people more than being a technology, It is integrating with many business system and development, to build trust of consumers. We require more cybersecurity professionals/ skilled people in many areas like financial services, aerospace firms, defense, government agencies, e-commerce, m-commerce, digital service agency, and, etc. Note that we required security solution for data at rest and data in motion [15]. Usually, a cybersecurity professionals are (will be) in near future:

- Identity Management,
- Endpoint Security,
- Data Security,
- Application Security,
- Securing our Email and Web,
- Compliance and Control Management,
- Manage Unified Threat,
- Incident Management,
- Secures Configuration,
- System Security, and Infrastructure.

Note that today national security and business interests of a country totally depend upon cybersecurity. So protect our nation form unwanted attacks, we require highly qualified person or cybersecurity professionals to avoid such cyber-crimes/ possibility of such crimes. Hence, this section discusses scope of cybersecurity and its related mechanisms in detail. Now, next section will discuss about necessity or requirement for finding vulnerabilities or attacks on software or embedded systems.

4. Necessity of Finding Vulnerabilities in Software/ Embedded Systems

Attacks designed to alter or knock out all or parts of systems. The final points are common ingredients innear future, some attacks designed to alter or knock out all or parts of systems. The final points are common ingredients in extreme scenarios such as cyber wars and terrorism, but are also methods employed by activists and bored hackers. The threats are increasing on all these fronts, but the same applies to awareness and technical aids.

Some government's initiatives like Digital India and demonetization have pushed companies towards digital transformation; doing so has also made them vulnerable to cyber-attacks. For that, we require security professions to find vulnerabilities in software/ public network, i.e., to achieve the digital transformation without compromising security. Also, we need some safeguards or secure mechanisms (also rules, policies, and regulations)for business's database from cyber-crimes. Hence, we need some stronger cyber laws and security systems to rectify/ find cybersecurity loopholes and take appropriate steps to protect their business/ organization from future threat/ vulnerabilities attacks.

Increase in criminal activities through computer network has led to the focus of attention towards protecting sensitive business and personal information, as well as safeguard national security. For example, WannaCry ransomware (attempted in 2017). In near future, cybersecurity will be tightly connected to the future of information technology (IT) and the advancements of the cyber-space. So, possibilities of attacks or threat over web will be more (i.e., higher). Most of internet connected devices will be integrated and will work almost in each and every possible application like driving, home automation, etc. But, breaching in such application may cause us more loss. As we discussed above sections an enemy country can defeat another nation just via implementing its cyber space strategy against its enemy. Any attacker can have access to "strategic weapons" that don't require the infrastructure or the cost of conventional weapons

One of major changes in challenges in cybersecurity is that many attackers use bots to infect other systems. But, such attacks can be prevented though via providing a complex and secure infrastructure. Note that complexity and connectivity of these systems directly impacts their level of vulnerability.

A cybersecurity analyst helps in planning, implementing and upgrading security measures and controls. They are also responsible for conducting vulnerability testing, risk analyses, and security assessments, and for managing the network. Hence, this section discusses reason or necessity behind detecting vulnerabilities or attacks on embedded systems (in present and future). Now, next section will discuss available techniques or methods to protect such attacks.

5. Available Techniques and Algorithms to Keep Information Safe and Secure on Web

There are several mechanisms used to protect against cyber-crime/ cyber-attacks. Some of them are strong password, firewall, using of Blockchain technology, threat hunting, digital forensics, intrusion detection process, etc. Few mechanisms are listed here as:

- By using a firewall, we can protect unwanted attacks on our systems/ infrastructure. A Firewall can be a software program or hardware device that filters the information and data coming from the public networks into a private computer system.

- Intrusion Detection System (IDS) [16]: An IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities.Note that it (IDS) also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

In detail, IDS can be discussed as:

Intrusion Detection System (IDS) provide monitoring system activity through examining vulnerabilities in the system and alert respective administrators. This is done through:

- System files comparisons against malware signatures.
- Scanning processes that detect signs of harmful patterns.
- Monitoring user behaviour to detect malicious intent.
- Monitoring system settings and configurations.

In signature-based detection, a pattern or signature is compared to previous events to discover current threats. Another type of detection is anomaly-based detection. There are three primary components of an Intrusion Detection System (IDS):

- Network Intrusion Detection System (NIDS): This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- Host Intrusion Detection System (HIDS): This takes a "picture" of an entire system's file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

Note that an Intrusion Prevention Systems (IPS) complements an IDS configuration by proactively inspecting a system's incoming traffic to weed out malicious requests. In general, a typical cyber-attack is an attempt by adversaries or cybercriminals trying to access, alter, or damage a target's computer system or network in an

unauthorized way. It is systematic, intended, and calculated exploitation of technology to affect computer networks and systems to disrupt organizations and operations reliant on them. This system scrutinizes the internet searching for any suspicious activities and gives an alert sound if found.

Internet of Things (IoT) [17] and Industrial Internet of Things (IIoT) [18] sensors and systems they enable are exponentially increasing the number of endpoints and threat surfaces an enterprise needs to protect. Now a days in healthcare, smart devices like internet connected things or internet of things are used. They have probability of tempering or hacking, and can be controlled by an unauthorized user. A patient can lose his/ her life due to such attacks on medical devices. Which is really a serious issue? Today' medical devices are susceptible to hacking, so require efficient mechanisms against cyber-attacks [19].Also to avoid any kind of breach/ attack on their systems/ network, users should be careful not to publish sensitive information on social media and adopt fundamental security solutions such as password protection, firewalls and antivirus software. Also, enterprises must implement security controls and train employees to use them.

Hence, this section discusses several available techniques and algorithms to keep information safe and secure on web (public network). Now, next section will discuss about several problems which has risen during protection or identifying / detecting vulnerabilities on a public network.

6. Problems Raised during Protecting Businesses (Software)Against Vulnerabilities/ Attacks

In the past decade, many companies/ users have reported instances of security breach by cyber-attack.For example, previously, SCADA (Supervisory Control and Data Acquisition is a control system architecture) [20] was secure by nature, inaccessible to outside parties using proprietary protocols, but due to reduction in cost and having more accessibility, it also became vulnerable. For such systems (complex), identity and password management are critical. Note that SCADA is a type of Cyber Physical System (CPS), a complex system to handle. Many issues and challenges related to cyber based physical system have been discussed in [21].

When a user receives a very aggressive phishing email, identity and access management system is informed that this user is under attack and they can then take that context, at that time user is unable to access its information and reveal its basic information to attackers (in hurry). Also, preventing its system against some attacks require some information/ awareness to uses software or protection mechanisms. Due to not having proper awareness, most of users loss or share their personal information to fraudsters/ attackers. For example, fraudsters call to bank's customer and request them to give their basic details to credit the winning lottery in their account. Customer does not much awareness about such attacks and shares his/ her details with the fraudsters. Such kinds of attacks are really difficult to prevent or stop.

Top Challenges with Cybersecurityare:

- **Ransomware Evolution:** Ransomware is the bane of cybersecurity, IT, data professionals, and executives.
- **AI Expansion:** Robots might be able to help defend against incoming cyber-attacks.Between 2016 and 2025, businesses will spend almost $2.5 billion on artificial intelligence to prevent cyber-attacks.
- **Internet of Things Threats:**Most people are always plugged in.
- **Blockchain Revolution:**2017 ended with a spectacular rise in the valuation and popularity of cryptocurrencies like Bitcoin and Ethereum. These cryptocurrencies are built upon Blockchains, the technical innovation at the core of the revolution, a decentralized and secure record of transactions. What does Blockchain technology have to do with cybersecurity?
- **Server-less Apps Vulnerability:**Server-less apps can invite cyber-attacks.

Hence, this section discusses many problems which raised in businesses/ sectors, using cybersecurity. Now, next section will discuss several opportunities for future research communities.

7. Opportunities for Future Research Communities

As discussed above, we find that main aim of cybersecurity is to secure digital information form malicious or unauthorized users**.** The future of cybersecurity cannot be considered without talking about emerging trends in technology and threat landscapes. As organizations develop and adopt technologies related to big data, cognitive computing and the Internet of Things (IoT), cyber threats are growing in both volume and complexity. Everyone is willing or in race to protect their business against such threat and attacks.61% of enterprises say they cannot detect breach attempts today without the use of AI technologies [22]. Fraud detection, malware detection, intrusion detection, scoring risk in a network, and user/machine behavioral analysis are the five highest ArtificialIntelligence (AI) use cases for improving cybersecurity**.**

Opportunities with Internet of Things (IoTs) in Cybersecurity

In this we need to secure the Internet of Things devices. Security professionals are well-versed in protecting servers and traditional mobile devices such as smartphones, but what about cars, refrigerators, thermostats and other home automation gadgets? Even more importantly, can they secure medical equipment in increasingly connected hospitals? Cybercriminals commonly hijack connected devices to form botnets in larger efforts to commit distributed denial-of-service (DDoS) [23] attacks against high-profile websites. It is becoming even more important for users and enterprises to properly secure their devices. Device manufacturers should build effective security controls into their products, and organizations should conduct exhaustive application security testing.

Opportunities with Cyber PhysicalSystems in Cybersecurity

In this section, we look to secure large scale infrastructure against cyber-attack. Many attacks have been mitigated and traced on cyber physical systems in the previous decade. In Cyber physical systems infrastructure, IoT has main functionality. However that, organizations are struggling to manage and monitor many user's records/ identities on SCADA. For that, password free-world can be a solution, which will be ruled (initiated) by Artificial Intelligence. Many threats are identifying everyday on big data and IoT, which related to (apply) the health-care industry as well. Industry 4.0 (Fourth Industrial Revolution) concerns about industry, having Cyber-Physical Systems (CPS) [24], the Internet of Things (IoT), Industrial Internet Of Things (IIOT), cloud computing, cognitive computing and artificial intelligence together. In near future, these all technologies have the potential to affect a series of systemic shifts in that landscape.

Opportunities with Artificial Intelligence (AI) in Cybersecurity

There are many opportunities can be seen with AI in near future, few are listed here as:

- Creating more accurate, biometric-based login techniques
- Detecting threats and malicious activities using predictive analytics
- Enhancing learning and analysis through natural language processing
- Securing conditional authentication and access

Security professionals can fight cyber-crimes/ cyber threats because every attack on web leave a digital trail. Security analysts can use this data to predict attacks and identify malicious actors before they strike. The process of analyzing millions of unstructured records, however, can take days. So 'cognitive security' comes into picture. With Machine Learning (ML), IT professionals can process threat data more efficiently, and more accurately predict criminal activity.

Hence, ransomware operators are particularly drawn to health care data because it is critical, difficult to secure and highly personal. Skilled people or expert in the security space should pay close attention to this highly

targeted industry. In summary, in healthcare, military, transformation, automation industry we have lot of opportunities in near future with respect to cybersecurity [21]. Hence, this section provide a complete scenario, i.e., future of cybersecurity with discussing many opportunities with IoTs, CPS, AI, etc., Now, next section will provide an open discussion which will provide that cybersecurity is the necessity of 21stcentury, for delivering efficient services, we require cybersecurity mandatory or some rules and regulation (implemented by government) to control cyber-attacks/ cyber-attacks on web (or internet related applications).

8. Open Discussion: Is Cybersecurity Really Required?

A large amount of data is produced by a rapidly growing number of smart or internet enabled devices. This data is available is structured and unstructured form. There are many ways to use this information in advertising and marketing campaigns, in analytics processes. Now think what will happen if cybercriminals or attackers got their control on this data? With such power to influence the public's behavior, the consequences could be dire. For example Cambridge Analytica had influence behavior of million people using analytics process (during US election in 2016).Also note that even the human brain itself can produce data for researchers to analyze. Scientists use sensors to understand how the brain reacts to certain stimulants and emotions in the interest of medical advancement. Such kind of information is highly required to researchers and malicious users (e.g., competitors in business) to move their next step.

Note that defending against 'strong' AI – where criminals use systems that operate, think and act as humans – and against 'weak' or 'narrow' AI – where systems are modeled on human behavior to execute specific tasks. Given its potential uses, AI is expected to drive systemic changes in the cybersecurity landscape, and will impact four key challenges in cybersecurity in the near future.

- Increasing sophistication of attackers
- Asymmetry
- Increasing the attack surface / Digitalizing operations
- Balancing risk and operational enablement

Cybersecurity Affects Everyone

Today's cybersecurity affects almost every business/ sectors, and IT professionals can rectify these vulnerabilities easily via using their intelligence. Also, when IoTs are also being used by all possible sectors in this 21stcentury (smart era), we need to more sincere about such serious/ dangerous cyber-crimes. Remember that cognitive computing, big data analytics [25] and the IoT (increasingly connected world)will develop and influence our society (surrounding environment) in unprecedented ways.

Hence, to avoid these attacks or protect ourselves against such attacks, organizations can do their part by sharing threat data and investing in solutions and infrastructures, i.e., secure by design its infrastructure. Also, users are suggested to use strong password and recommended to avoid opening a suspicious or unsolicited emails and attachments. Hence, this section provides an interesting open discussion about using of cybersecurity in smart era/ 21stcentury. Now, next section will conclude this work in brief with some interesting knowledge/ facts (research gaps) related to cybersecurity, recommended to researchers to read.

9. Conclusion

Today's many threats or attacks are changing the way of doing businesses in 21stcentuary. Every business manworries about cybersecurity attack. For that, we proposed a complex environment for industries/ organizations to secure, i.e., encrypting information using Blockchain Technology or with having strong password, etc. Apart from this, there are many areas which require high attention in the cyber-security space,

but we (researchers) do not look at them. For a tighter security (for a cyber infrastructure), we need to work on concept like Defense-in-Depth. Also, we require cognitive security (computing) to shape the future of cyber-security. Together this, powerful developing technologies like AI, 5G, biometrics and new encryption technologies will change the landscape of cybercrime for both attackers and defenders.

In summary for future, Organizations must defend against cyber-attacks/ vulnerabilities, as well as their partners in both the public and private sectors. Also, they need to work together in Public-Private Partnerships (PPP) to catch/ get "how new technologies will change the risk and threat landscape, and to prepare a collective, adequate response". Also, government can implement some regulations to protect data in near future to avoid some rate of cyber –attacks (inside a country). Hence, all covered suggestions, or methods are required to be implemented in near future by people/ researchers who are working related to this area in an efficient and cheaper/ affordable ways.

Acknowledgement

This research work is funded by the Anumit Academy's Research and Innovation Network (AARIN), India. The authors would like to thank AARIN, India, and a research network for supporting the project through its financial assistance.

References

1. A. Gandomi & M.Haider, "Beyond the hype: Big data concepts, methods, and analytics", International Journal of Information Management,35(2), 137–144, 2015, doi:10.1016/j.ijinfomgt.2014.10.007

2. P. Wang, L.Wu, R. Cunningham & C. C. Zou, "Honeypot detection in advanced botnet attacks", International Journal of Information and Computer Security, Vol. 4, No. 30-52, 2010

3. C. Palmer, "Ethical hacking", IBM Systems Journal, 40(3), 769–780, 2001 , doi:10.1147/sj.403.0769

4. K. Ashok , P.Shweta & A.Praveen , "The WannacryRansomeware, a Mega Cyber Attack And Their Consequences On The Modern India", International Journal of Management Information Technology and Engineering, Vol. 6, Issue 4, 1-4, 2018.

5. N.B. Sukhai, "Hacking and cybercrime", Proceedings of the 1st Annual Conference on Information Security Curriculum Development - InfoSecCD '04. 2004. doi:10.1145/1059524.1059553

6. https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

7. N. Jovanovic, C. Kruegel & E. Kirda, "Pixy: a static analysis tool for detecting Web application vulnerabilities. in Security and Privacy", 2006 IEEE Symposium on , vol., no., pp.6 pp.-263, 21-24 May 2006 doi: 10.1109/SP.2006.29

8. J.M. Chen & C. L. Wu, "An automated vulnerability scanner for injection attack based on injection point", Computer Symposium (ICS), 2010 International, pp.113-118, 16-18 Dec. 2010.doi: 10.1109/COMPSYM.2010.5685537

9. M.E.Ruse, & S.Basu "Detecting Cross-Site Scripting Vulnerability Using Concolic Testing. in Information Technology: New Generations (ITNG) ", 2013 Tenth International Conference, pp.633-638, 15-17 April 2013 doi: 10.1109/ITNG.2013.97

10. M.K. Gupta, M.C. Govil & G. Singh, "Static analysis approaches to detect SQL injection and cross site scripting vulnerabilities in web applications: A survey", Recent Advances and Innovations in Engineering (ICRAIE), vol., no., pp.1-5, 9-11 ,May 2014 , doi: 10.1109/ICRAIE.2014.6909173

11. Z.J.Wang, Y. Liu & Z.J.Wang, "E-mail filtration and classification based on variable weights of the Bayesian algorithm", AppIMech Mater, 513–517:2111–2114, 2014.

12. W.C. Hsu, & T.Y. Yu , "E-mail spam filtering based on support vector machines with Taguchi method for parameter selection", J ConvergInfTechnol, 5(8):78–88, 2010

13. G. Caruana G, M.Li & M. Qi , "A MapReduce based parallel SVM for large scale spam filtering", In: IEEE 2011 eighth international conference on fuzzy systems and knowledge discovery (FSKD), 2011; pp 2659–2662

14. Z. Zheng, S. Xie, H. Dai, X. Chen & H.Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), 2017

15. A.K. Tyagi, G. Rekha, & N.Sreenath, "Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns", In: S. Satapathy, K. Raju , K. Shyamala., D. Krishna, & M. Favorskaya. (eds) "Advances in Decision Sciences, Image Processing, Security and ComputerVision", ICETE 2019.Learning and Analytics in Intelligent Systems, vol 3. Springer, Cham.

16. H.J. Liao, C.H. Richard, Y.C Lin & K.Y Tung, " Intrusion detection system: A comprehensive review", Journal of Network and Computer Applications, 36(1),16–24, 2013, doi:10.1016/j.jnca.2012.09.004

17. E.Hodo, X. Bellekens, A. Hamilton, P.L. Dubouilh, E.Iorkyase, C.Tachtatzis, & R.Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system", 2016 International Symposium on Networks, Computers andCommunications(ISNCC),2016,doi:10.1109/isncc.2016.7746067

18. A.R. Sadeghi, C. Wachsmann, & M. Waidner, "Security and privacy challenges in industrial internet of things", Proceedings of the 52nd Annual Design Automation Conference on - DAC '15.2015. doi:10.1145/2744769.2747942

19. M. Shamila, K. Vinuthnaand T.K.Tyagi," A Review on Several Critical Issues and Challenges in IoT based e-HealthcareSystem".International Conference on Intelligent Computing and Control Systems [ICICCS 2019], IEEE, 2019

20. C.W.Ten, C.C. Liu, & G.Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems", IEEE Transactions on Power Systems, 23(4), 1836–1846, 2008, doi:10.1109/tpwrs.2008.2002298

21. A. K. Tyagi, "Article: Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cybersecurity", International Journal of Computer Applications 137(14):19-27, March 2016. Published by Foundation of Computer Science (FCS), NY, USA.

22. M.K. El-Najdawi &A.C. Stylianou, " Expert support systems: integrating AI technologies", Communications of the ACM, 36(12),55–59, 1993, doi:10.1145/163298.163306

23. F.Lau, S.H. Rubin, M.H. Smith,& L.Trajkovic, "Distributed denial of service attacks" , SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics. doi:10.1109/icsmc.2000.886455

24. E.A.Lee, "Cyber Physical Systems: Design Challenges", 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC).2008. doi:10.1109/isorc.2008.25

25. https://vivomente.com/wp-content/uploads/2016/04/big-data-analytics-white-paper.pdf

Appendix A

Table 1: Cybersecurity Tools and Their Uses

Sl No	Cybersecurity Tools	Description
1	BluVector	Provide protection for the machines with the help of AI and Deep learning. It can be installed either as a hardware based network appliance or as a virtual a machine.
2	Bricata	Advanced technology with multiple detection engine which can launch automatic threat hunts based on the events occur in the organization
3	Cloud Defender	Work efficiently in cloud environment. It is a user-friendly tool which enables the staff to identify the breaches in the cloud easily.
4	Cofense Triage	Efficient tool against phishing attacks. Deep learning and AI implementation enable this tool to learn from previous attacks which already occur.
5	Digital Guardian	It provide ready to deploy end point security.
6	Intellicta	It is used to tackle issues related to compliance rule.
7	Mantix4	Provide robust threat hunting tool in one complete package.
8	Contrast Security	It is a suite of tools, which protect the application from inside out.