TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

Cyber-hygiene: The key Concept for Cyber Security in Cyberspace

[*]Debabrata Singh[1], Namrata P. Mohanty[2], Shrabanee Swagatika[3], Santosh Kumar[4]
[2,3]Dept. of CSE, ITER, Siksha 'O' Anusandhan University, Bhubaneswar, India
[1,4]Dept. of CSIT, ITER, Siksha 'O' Anusandhan University, Bhubaneswar, India

*Corresponding Author: -debabratasingh@soa.ac.in

Article Info
Volume 83
Page Number: 8145 - 8152
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

Abstract:

Internet has become the backbone of this modern world. Though internet has brought the world as close as a click away from our fingertips still there are a lot of issues in this world of cyberspace. Cyberspace is the environment where various devices and equipments are interconnected to each other and are used widely in our day to day lives making it a lot easier to deal with. In order to keep the cyberspace clean both from inside and outside it is necessary to maintain specific rules and regulations like 'Cyber-hygiene'. This paper explores the various aspects of the cyberspace, issues that arise while we deal in the world of cyberspace and how to maintain proper cyber-hygiene so keep individuals as well as a group of organizations safe from different cyber attackers, cyber threats and cyber-risks. From our study we find that Cyber Hygiene will provide a better protection, better security and also in monitoring and maintenance of the networks.

Keywords:*CIS-Centre for Internet Security, CCS-Council on Cyber Security, Cyberspace, Cyber threats, Cyber attack.*

1. Introduction

Cyber-hygiene refers to maintain proper norms and guidelines in the cyberspace in order to protect data from attackers. Now-a-days we can see the increase in cyber-threats vividly in the cyber-world. Starting from an individual to a group of organization each and everyone needs to maintain cyber-hygiene to keep them saves from the spasm, virus attacks, etc. As indicated by the CIS (Center for Internet Security) and CCS (Council on Cyber Security) digital cleanliness is characterized as "Means to appropriately protect and maintain IoT systems [1] and devices and implement cyber security practices [2]". The Defense department adopted the good cyber security techniques for free computer malware [3]. It also maintains Cyber hygiene at all time and helps reducing insider threats. Now a day's cyber attacks frequency increases on healthcare systems as well as financial industries. A recent ASIC (Australian Securities and Investments Commission) reported that industry system must be tightened for financial services and other services i.e. "Cyber-resilience health-check"[4]. The important organization must be concerned about unprecedented cyber attacks, which grow rapidly over different area like mobile, Internet, data-driven, and cloud services. Mainly cyber criminals and hackers induce different types of malware to their victims. Recently a dangerous malware, ransomware blackmail for crash the victim's computer. Crypto-ransomware is another one has become popular for extract money from victim's inadvertently downloading the malware. This new variant of malwares helps to the cyber criminals to attack on individuals as well as organizations [5].

Remaining part of the paper systematized as follows; in Section 2 we describe the concept of cyber hygiene with proper explanation of cyber attacks. In Section 3 we review some of the literature about cyber hygiene. In Section 4 we represent the types of threats and their control measure with some cyber threats and cyber attacks. In section 5 we presented how to regulate the cyber security by the help of cyber hygiene. In last section we conclude our paper with some references.

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

2. Cyber Hygiene

In this era of 21st century which is better known as the digital era, where we can't even imagine our lives without the internet, there is also an aspect called the cyber-hygiene which is closely associated with the internet and without which probably we can't rely on this internet fully [6]. No doubt internet has made our lives much easier than before; we can say literally it has brought the world to our finger tips. Starting from carrying out all necessary household jobs to working in our professional sectors, Internet has done everything a lot more easily [7]. For example, right from filling up the bills of electricity, water to filling of home loans of lakhs everything can be done by just sitting at the home and accessing the internet. At the same time if we don't consider some really necessary norms then everything has surely a risk of falling in the hands of cybercriminals and all our personal and professional data will be available to them within seconds [8]. This paper will enlighten us about the most important aspect related to the era of internet and that is the cyber-hygiene. Cyber attacks mostly occur through the cyberspace and the cyber applications only. Let's have a look on the steps through which these cyber-attacks are mainly carried out as depicted in Figure 1.

i.Recon: The attacker finds the weakest link in the victim's device or the system software.
ii.Intrusion & Presence: In this phase the attacker establishes connection through the link with targeted victim's software without the knowledge of the victim and injects the malware to the victim's system.
iii.Lateral Movement: The attacker tries to find the targeted data in the victim's system by establishing connection with the internal network of the victim's device.
iv.Privilege Escalation: Here the attackers use false identification to gain the necessary privileges in order to extract data from the victim's device or the system software.
v.Mission Complete: The attacker reaches the final stage and extracts the data from the victims system and corrupts and disrupts all the activities that have been carried out in the victim's computer.

Cyber mess-In current data information system which builds the digital hazard factor or an information rupture is called as cyber mess [9]. This cyber mess can be arranged into two classifications i.e. technical and non-technical.
The technical digital hazard occurs due to the absence of following:

i. Authentication, authorization and accounting
ii. Security Monitoring and its intelligence
iii. Access control like data level and function level
iv. Incident response plan (accidental)
v. Continuation of risk assessment and risk factor management

The non-technical cyber mess occurs due to the absence of following:

i. Security awareness
ii. Organization policies
iii. Ignorance
iv. Employees training
v. Social engineering awareness.

2.1. Working principle of Cyber Attacks

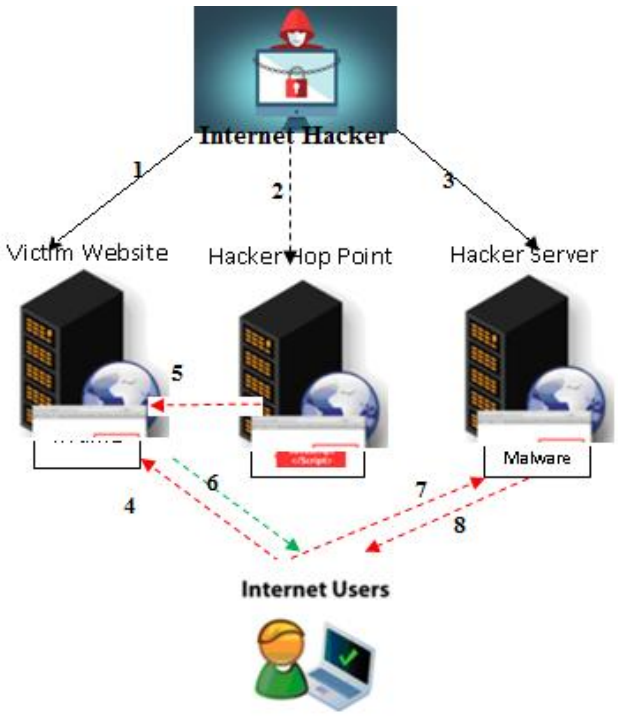

Figure 1: Cyber attack (Source: https://resources.infosecinstitute.com /the-importance-of-cyber-hygiene-in-cyberspace/#gref)
Cyber attack can be operates in three major steps as depicted in Figure 1 and all eight steps are described below.
A) **Internet Hacker's activities:**

i. Inject malicious iframe to the victims vulnerable website
ii. Exploit the Java script values on hacker control website

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

iii. Next hacker controlled server planted the malware

B) **Legitimate the web usage:**

i. General Internet user requests victim's web-page, which opens malicious iframe, without taking consent.

C) **Malware path Infection:**

i. In web browser, malicious iframe executes & exploit the codes.
ii. Exploit browser vulnerabilities to take the control & instruct to download the malware.
iii. From hackers server , browser silently request malware.
iv. Malware then silently install & execute it's operation on user's Internet.

3. Literature Review

In order to know the different cyber-hygiene practices first of all we need to be aware of different cyber threats that arise in the cyberspace .The two well known organizations CIS and CCS both jointly launched a cyber-hygiene campaign aiming at providing immediate and effective defences against cyber-threats at a comparatively lower cost. J.A. Oravec et al. [10] represents the "Developing cyber hygiene practices for the Internet of Things (IoT): Professional issues in counseling customers and instructing clients on IoT protection and security" throws light on the issues arising out of cyber-threats and cyber-attacks and at the same times shows how cyber-hygiene can combat this effect in the field of Internet of Things(IoT) and cyberspace as well. This paper also discusses the roles of various professionals such as doctors, lawyers, teachers, consultants, marketers, etc in reducing the effect of cyber-attacks by adopting to certain useful cyber-hygiene practices. This paper also explores various measures by which cyber hygiene can be maintained by all groups of people dealing in the world of cyberspace for carrying out their respective jobs or tasks. J. A. Chaudhry et al. [11] described in thier research paper about "Phishing: Classification and Countermeasures" and also discussed about various hybrid problems involving both technical and social issues arising from phishing attacks. This paper also explores the efficient measures to combat the effect of these attacks. It also discusses technical as well as practical methods so as to defend against these attacks by hardening the infrastructures and by making the employees as well as usersaware against such attacks. In reference R. Savold et al. [12] introduced the concept "Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks" and also discussed the need to build an agile structure in the field of cyber-hygiene and cyber-security in order to develop the informing procedure of such unknown threats, fraudulent activities for the users which makes them aware about these attacks from a much before time so that they can get enough time to reduce the effect of those attack to much lower extent. H.Kimiyama et. al. [13] throws light on how cyber attacks put adverse impacts in the world of cyber space. The author takes into consideration the DDOS attack that happened in the year 2016 that used "Mirai botnet" and generated 600gbits/traffic which is much more the traffic generated in the previous years. The author also proposed an Artificial Intelligence System(AIS) infrastructure that helps in securing the data in the cyberspace to a large extent as well as proposed 3 multilayer binding routers to carry out the security functions by the infrastructure and also shows how all the malicious activities can be filtered by his proposed AIS infrastructure. W. Ding et.al.[14] focus the light on how the current world is facing the security challenges and cyber attacks as well proposed designs which should be taken into consideration in order to make the world of cyberspace more clean and secured.

4. Types of Cyber Threats and Their counter Measures

There are mainly 6 types of cyber threats that arise in the world of cyber space. Let's have a discussion on these 6 types of threats and the countermeasures of mitigating them to a large extent.

i. Social Engineering: It refers to attacking the "weakest link" in the security chain by psychologically manipulating the people for performing actions or divulging confidential information by techniques such as phishing, "dumpster diving" or even personal blackmailing [15][19]. It's the main reason why even well equipped and security aware companies falls as victims in the hands of cyber attackers. Cyber criminals are always on a mission of finding the weakest link in security chain through which they can insert the virus or the malicious software to the targeted victim's system. Therefore it is necessary to find and secure the weakest link in the software security chain. Some of the initial actions that

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

can be taken to combat such attacks include blocking network connections to malicious content, blocking Wi-Fi connections to unsecured networks, stop using malicious web-pages and websites and performing activities on them. Other approaches including patching vulnerable systems, mitigating known threats in the application, keeping your devices up-to-date with the latest version, etc need to taken in order to reduce such attacks.

ii. Attacks on Hosted Components: These attacks includes malicious software injection to the targeted system such as SQL injection, cross –site scripting, etc and other techniques that threatens the access and authentication controls in cloud based control systems which handles large no. of sensitive data [16]. Here,the control-measures mostly include API authentication, role based approaches, creating awareness to protect against 'impersonation' at cloud level,etc.

iii. Hacked Device Software: When the attacker gains access to the software at device level then it carries out a lot of techniques and fraudulent activities including malware injection, denial of service, false identification, elevation of privileges, etc to take control over the data present in the system [17]. We can combat this types of attacks by carrying out techniques such as "secured boot" which means when any fraudulent activities is carried out in the system then normally after rebooting the system doesn't turns on thus all the data present in the systems becomes safe from the attacker, software update that is keeping the system and the its software up-to-date with the latest version available, software isolation, etc.

iv. Physical Attack: This type of attack is mostly carried out in the area where a lot of IOT applications is used as IoT applications are connected with a lot of hardware devices and components which are located far away from each other and can't be monitored at a single location easily and thus hackers can easily hack these devices [18]. The major counter measures here includes file system encryption which means proper encryption decryption techniques and algorithms must be used so that the data can be secured properly, trusted platform modules enables to store the data on different platforms securely, remote attestation means attesting a remote to each far away hardware devices so that it can be controlled from faraway places as well.

v. Network Compromise: These types of attacks are known as 'middle way attack' where the attackers mostly use techniques such as session hijacking to enter a network to disrupt ,block or alter communications between the devices and their cloud based controller. Here the control measures includes proper file encryption and decryption techniques to be used while sending and receiving data between the end-to-end user, keeping the software updated, etc

vi. Security Mis-configuration: Many a times due to some carelessness or inattentiveness while handling the security changes of the software, the security changes become misconfigured and thus providing the hackers with an opportunity hack the devices and extract the data from it. So security changes should be carried out with utmost care with proper encryption decryption techniques as well [19].

4.1. Lack of Cyber Hygiene Leading to Cyber Threats and Cyber Attacks

A cyber-attack named WannaCry [20] Ransomware attack which came few years back attacking the Microsoft Windows operating system on a large scale including windows 8, 2003 and XP users as well. Because of the reason that a lot many people and organizations had not updated their software security version as per the month of March whereas the latest version had been released in 2014 itself. Due to this reason unlicensed windows software, systems having out-dated software versions became more vulnerable to this attack. This particular affected a lot of business institutions, hospitals, banking and corporate sectors from all over the world. Computes, MRI Scanners, CT Scanners, databases were affected in the hospitals. In banking and corporate sectors, computers having transaction databases had been affected severely by this cyber-attack. Around 200,000 to 300,000 estimated computer systems were affected in approximately 150 countries. Generally cyber attackers/criminals are targeting billionaire, Government departments, defense department and Web site of big industries/big companies.

Ransomware [21] is a cyber malware, which blocks the data access and related information. It contaminated through the access over data with vulnerable ports (SMB). Sometimes it needs a n amount to be

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

paid for accessing the infected data and when the user clicks on that link or attachment it actives on that email.It can also in filter the system when the user visits some websites or some web-pages inside the websites. This cyber malware encrypts according to itself, blocks the internal files and make them inactive or inaccessible for the end user. It also infects the server attached to that system and sometimes also locks up the whole computer network systems.

In this procedure first of all, the attacker generates a key pair and places the corresponding public key in the malware and then the malware is released. After that the malware generates a random symmetric key which then encrypts the user's data with it .This is known as hybrid encryption in which it uses the public key in the malware to encrypt the symmetric key and this results in the formation of small asymmetric ciphertext and symmetric ciphertext of the user's data as well. It also puts up a message to the user including the asymmetric ciphertext and a ransom amount which is supposed to be paid by the user in order to get rid of this attack. If the user sends back the asymmetric ciphertext along with the e-money or the ransom amount to the attacker, then the attacker deciphers the asymmetric ciphertext with the attacker's private key and sends the symmetric key back to the users after which the user will be able to decipher the encrypted data with the help of the symmetric key. And in this way this crypto virological attack will be completed.

Though there are no such records of computers getting decrypted after making the required payments still this attack was mitigated by Marcus Hutchin battles accusations of involvement in a malware scam, which discovered a "kill switch" which was coded in the malware itself [22]. He enrolled a space name for the DNS sinkhole(a DNS which gives false data about a domain),and halted the spreading of the infection like a worm, accordingly backing off the spread of malware and offering time to the clients to concoct protective measures. Then another person named Adrian Guinet created a "wannakey" which was a solution to the WannaCry Ransomeware based on its flaws ,provided that the infected computer was not being rebooted or the decryption key was not overwritten by the malware [23]. This is just an example of showing how a little ignorance in cyber-hygiene could lead to severe cyber-attacks and cyber threats [24-25]. Some of the prevention should be taken i.e. delete cookies regularly, activate Google Opt-Out while logged into Google to avoid unwanted search, use credit cards & PayPal cards instead of debit cards, put a hard drive to back up the data, turn off the Google's web history and bring counterfeit for any online purchase. If the users would have updated their software in due period of time then such major attacks could have been avoided easily and efficiently.

5. Various Campaigns And The Cyber Security Threats

There are mainly two associations namely the CIS and CCS are responsible for regulating the security aspect of all IT systems and devices[26]. The vision over here is providing low cost immediate and effective cyber-hygiene practices against cyber attacks. It creates awareness by organizing various campaigns and the practices includes the below steps mainly:

Count- Knowing your own connection and the devices that are connected to your system.

Configure- Implementing the security settings to protect your system thoroughly.

Control- Managing the security settings about the various visibility aspects of the system.

Patch- Keeping the device and the system software's up-to-date.

Repeat-Revise and re-visit the top priorities for a solid foundation of cyber security.

Generally different kinds of cyber security threats are:

1. Bring your own device(BYOD) policies: Using personal devices infected with a virus at work can easily compromise the organization's as well.
2. Shadow IT systems: Usually, these IT systems are not compactable with an organization's central IT system. AS a result data loss and security threat keep rising.
3. DDOS: The distributed denial-of service attack floods the organizations network with traffic and ultimately shuts it down.
4. Malware Attack: Malicious software programs can get ahold of your sensitive information without you, even noticing.
5. Flaws in Internet of Things(IoT): Devices connected through a flawed Internet of things is more to security issues.
6. Inside Man: Bad players within an organization can easily breach security because of easy access.

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

7. Crypto-Malware: This malware get access to your computers processing power and use it to mine crypto-currencies.
8. Phishing E-Mail: It contains the Trojan horse or ransom-ware viruses. 97% of the people can't tell the difference and open it, releasing the virus.
9. Data Breach: Many use obsolete data storage networks that are prone to data breaches.
10. Insecure Application user Interface(API): The lack of proper security measures in the application user interface can cause security breaches.
11. Fileless Malware: This malware don't exist as a file in the hard-drive and work in the background.
12. Stegware: Stegware are malicious files hidden within another file, such as Video, image, messages etc.
13. Cloud abuse: Most of the cloud storage can be accessed by hacking the virtual machine.
14. Single factor passwords: Using only a single factor password is not enough to offer full security till date, because they are easy to crack.
15. Zero day Threats: Most of the programs come with security holes and cyber criminals find this security lopes and use it.
16. Whaling: It's a form of phishing attack, where the attacker convinces to be reliable, but latter abuses the data.

5.1 Best Practices in Cyber Hygiene

The guideline of digital cleanliness centers on breaking any progression in the digital assault chain, which thusly will effectively keep the assault. Basic security preparing programs are not only adequate to battle the assaults that occur in the realm of the internet. Thus, obstructing the underlying phishing messages, blocking system associations with known pernicious substance, and halting malevolent process action are basic to battling digital dangers. The genuine test lies in deciphering mind boggling and specialized digital information into down to earth data which can be effortlessly comprehended by the business and also the security experts. Digital cleanliness incorporates fundamental advances like fixing helpless frameworks, diminishing known dangers in applications, solidifying servers and system sensors.

Individuals as well as group of organizations must adopt certain policies[27] and practices to recognize the weakest connections and security escape clauses. Actualizing security at each level from application improvement, foundation solidifying, arrange checking, Bring Your Own Device (BYOD) approaches [28], to representative mindfulness is urgent part in taking care of the security issues i.e.

i. **Identify:** Distinguishing every last gadget that is associated with the web. Each gadget that is associated with the web is defenseless against digital assaults and gets digital dangers at consistent interims. It makes an assault surface and a passage point for the digital crooks.
ii. **Prioritize:** Devices and applications should be ranked and categorized based upon sensitivity and data exposure. It also reduces the workload for the system administrators and security engineers.
iii. S**ecurity Hardening:** Gadgets, frameworks and applications must be solidified to secure and decrease the section point for a digital assault. It consolidates encryption of information, vulnerability assessments, secure configuration audits password policies, and two-factor authentication [24][29].
iv. **Security Patches:** Executing patch and weakness administration in all gadgets and frameworks is security Patches[30]. As indicated by a Verizon 2015 information breach investigation report, numerous existing vulnerabilities stay open, principally in light of the fact that security fixes that have for quite some time been accessible were never actualized. Actually, a significant number of the vulnerabilities are followed to 2007, a hole of very nearly eight years.
v. **Backup:** Organizations must execute a decent reinforcement arrangement. Customary reinforcement of critical information is a piece of a decent reinforcement technique for information security. It is the last safeguard against information misfortune or information burglary. Fusing an information recuperation process will guarantee that you can really recoup information from your reinforcement.
vi. **Effective training:** Effective training is the most cost effective training in cyber hygiene practices.As per the European Network and Information Security Agency, "Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks."The weakest link in cyber security is the people around us involved in cyber space and effective training begins with a person only which involves customer and staff educa-

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

tion, customer education program on spotting threats and so on and so forth.

5.2High Level control objectives and foundational Cyber Hygiene tasks:

Five Key cyber hygiene control objectives are 1. Protect the networks 2. Protect the perimeter 3. Protect the individual devices 4. Use the secured cloud and 5. Protect the supply chain.

The foundational Cyber Hygiene Tasks are described as follows: 1. Have a record of all hardware so you know what your estate looks like. 2. Have a record of all software to ensure it is properly patched or not. 3. Manages data in and out of your network. 4. Utilize secure configuration or hardening guides for all devices. 5. Scanning incoming emails. 6. Minimization of the admin accounts. 7. Regular back up of data. 8. Setup an incident plan record. 9. In supply chain give more security level 10. In cloud environment, provide security control service agreements.

6. Conclusion

According to Yaacob Ibrahim, Singapore's Minister of communication and Information "We need individuals to practice good cyber hygiene and safe surfing habits at work and at home, and we need all organizations to take ownership of your systems' and play your part". Cyber Hygiene distinct from cyber security, but it relates to each and single individuals rather than a group of organization. While cyber-hygiene is the responsibility of an individual, cyber-security is the responsibility of a group or organization and applies to their professional activities only. In this paper we throws light on various necessary practices that should be carried out by individuals as well as groups of organizations and implemented with continuous monitoring and mitigation analysis in order to achieve effective defenses against cyber-attacks and cyber threats. Hence, cyber-hygiene is a must in the world of cyberspace.

References

[1] B. D. Weinberg et al., "Internet of Things: Convenience vs. privacy and secrecy", Bus. Horizons, Vol. 58, no. 6, pp. 615-624, 2015.

[2] E. Holm, "The role of the refrigerator in identity crime", Int. J. of Cyber-Security and Digital Forensics, Vol. 5, no. 1, pp. 1-9, 2016.

[3] J. Angwin, "Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance," Colorado Technology Law J., vol. 12, pp. 291-308, 2014.

[4] O. Arias et al., "Privacy and security in Internet of Things and wearable devices", IEEE Transaction on Multi-Scale Computer System, Vol. 1, no. 2, pp. 99-109, 2015.

[5] L. Billingsley and S. A. McKee, "Cyber security in the clinical setting: Nurses' role in the expanding "Internet of Things", The J. of Continuing Educ. in Nursing, vol. 47, no. 8, pp. 347-349, 2016.

[6] http://www.bizmonitor.com.au/financial-services-face-cyber-attacks/

[7] http://securityaffairs.co/wordpress/34502/security/cyber-hygiene-principles.html

[8] http://www.tenable.com/blog/implement-good-cyber-hygiene-with-continuous-network-monitoring

[9] https://business.f-secure.com/5-phases-of-a-cyber-attack-the-attackers-view

[10] Oravec, Jo Ann., "Emerging "Cyber hygiene" practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security", In Professional Communication Conference (ProComm), 2017 IEEE International, pp. 1-5, IEEE, 2017.

[11] Chaudhry, Junaid Ahsenali, and Robert G. Rittenhouse, "Phishing: Classification and Counter Measures", In Multimedia, Computer Graphics and Broadcasting (MulGraB), 2015 7th International Conference on, pp. 28-31, IEEE, 2015.

[12] Savold, Risa, Natalie Dagher, Preston Frazier, and Dennis McCallam, "Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks," In Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on, pp. 127-138, IEEE, 2017.

May – June 2020
ISSN: 0193-4120 Page No. 8145 - 8152

[13] H. Kimiyama et al., "Autonomous and distributed internet security (AIS) infrastructure for safe internet", 2017 8th Int. Conf. on the Network of the Future (NOF), pp.106-113.

[14] W. Ding, Z. Yan and R. H. Deng, "A Survey on Future Internet Security Architectures", IEEE Access, vol. 4, pp. 4374-4393,doi: 10.1109/ACCESS.2016.2596705, 2016 .

[15] https://en.mwikipedia.org/wiki/social_engineering (security).

[16] Prakash, Pawan, Manish Kumar, Ramana Rao Kompella, and Minaxi Gupta, "Phishnet: predictive blacklisting to detect phishing attacks", In INFOCOM, 2010 Proceedings IEEE, pp. 1-5. IEEE, 2010.

[17] Raleigh, Gregory G., James Fitzgerald, Nathaniel Hunsperger, James Lavine, Vien-Phuong Nguyen, and Jose Tellado, "Service Processor Configurations for Enhancing or Augmenting System Software of a Mobile Communications Device", U.S. Patent Application 14/083,324, filed March 13, 2014.

[18] Sung-Ming, Yen, Seungjoo Kim, Seongan Lim, and SangJae Moon, "A countermeasure against one physical cryptanalysis may benefit another attack", In International Conference on Information Security and Cryptology, pp. 414-427. Springer, Berlin, Heidelberg, 2001.

[19] Hongsong, Chen, Fu Zhongchuan, and Zhang Dongyan, "Security and trust research in M2M system", In Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on, pp. 286-290. IEEE, 2011.

[20] Ehrenfeld, Jesse M, "Wannacry, cybersecurity and health information technology: A time to act", Journal of medical systems, Vol- 41, no. 7, 104, 2017.

[21] https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

[22] www.independent.co.uk/news/uk/home-news/marcus-hutchins-arrested-latest-us-authorities-wannacry-cyberattack-nhs-las-cegas-mccaran-a7875761.html

[23] https://twitter.com/adriengnt/status/865209689809747968?lang=en.

[24] M. Rader, S. Rahman, "Exploring Historical And Emerging Phishing Techniques And Mitigating The Associated Security Risks", *Int. J. Netw. Secur.*, 2013.

[25] Akankshya Aparajita, Shrabanee Swagatika, Debabrata Singh, "Comparative Analysis of Clustering Techniques in Cloud for Effective Load Balancing", International Journal of Engineering &Technology(IJET), Vol 7, No 3.4 (2018): Special Issue 4, pp.47-51, 2018.

[26] Kar, Binayak, Asif Uddin Khan, Laxminath Tripathy, Priyabrata Sahoo, and Raj Kumar Parida, "ECC Based Self Proxy Signature Scheme", In International Conference on Instrumentation, Measurement, Circuits and Systems (ICIMCS 2011). ASME Press, 2011.

[27] Banerjee, Arko, Bibhudendu Pati, and Chhabi Rani Panigrahi, "$$ SC^ 2$$: A Selection-Based Consensus Clustering Approach", In Progress in Advanced Computing and Intelligent Engineering, pp. 177-183. Springer, Singapore, 2018.

[28] Song, Yanjie. "Bring Your Own Device (BYOD) for seamless science inquiry in a primary school", Computers & Education74, pp.50-60, 2014.

[29] Wang, Shuzhen, Zonghua Zhang, and Youki Kadobayashi, "Exploring attack graph for cost-benefit security hardening: A probabilistic approach", Computers & security 32, pp. 158-169, 2013.

[30] Mulliner, Collin, Jon Oberheide, William Robertson, and Engin Kirda. "Patchdroid: Scalable third-party security patches for android devices", In Proceedings of the 29th Annual Computer Security Applications Conference, pp. 259-268. ACM, 2013.