LGURJCSIT
Volume No. 1, Issue No. 4 (October- December), pp. 37-50

AN OVERVIEW ON CYBER ATTACKS AND ITS TYPES FOR ENHANCING DATA SECURITY IN BUSINESS WORLD

Noor-Ul-Qamar, Kamran Mustafa, Eisha-Tur-Rehman, Shan-e-Zahra

Abstract*:* For sensitive data of organizations there is a compelling need of ensuring privacy in several aspects and to inculcate protective measures in systems especially in various high-tech firms. Cyber-attacks are a wide form of threat confronted globally on the web by several users on daily basis. These attacks are fundamentally used to challenge system security of others, there are likewise some moral programmers who get into other people frameworks to make them aware about their vulnerabilities and they also get paid in return for securing such systems. In any case, these assaults have caused a great deal of concern for businessmen. This research covers the major types of cyber-attacks that can affect the business world in an immense manner along with an overview that how these threats work and how they can be possibly prevented. As the hacking mechanisms are showing signs of increased danger in a step by step manner, our frameworks should also take preventive measures to remain safe from all sorts of latest attacks on our data that can possibly attack in various forms.

Keywords: *Computer Network Attack, SQL Injection, Phishing, Reconnaissance, SSL Attacks, Denial of Service*

[1,2,3,4] Lahore Garrison University

1. INTRODUCTION

A cyber-attack is an intentional misuse of personal computers on the technology-dependent corporations, companies and systems or sites. Cyber-attacks use harmful and destructive code to change coding of computer, reasoning or data, leading to disruptive effects or repercussions that can destroy the actual data and leads to cyber[5]crimes, such as identity or personal information theft. Cyber-attack is also called Computer Network Attack (CNA). Cyber-attacks can include the following outcomes:

- **a)** Extortion, fraudulence or identity theft.
- **b)** Spoofing, pharming and several others like malware, phishing.
- **c)** Hardware is being stolen, such as laptop computers or cellular devices.
- **d)** Denial-of-service and allocated denial-of-service attacks.
- **e)** Website defacement
- **f)** System infiltration
- **g)** Password sniffing
- **h)** Exploitation of personal and general public browser
- **i)** Instant messaging abuse
- **j)** Unauthorized access or intellectual robbery (IP) robbery

The Institute for Security Technology Studies at Dartmouth University investigates and studies cyber-attack issues arising in police investigations and targets the constant development of IP tracing[1], real-time interception nationwide, data sharing and data evaluation.

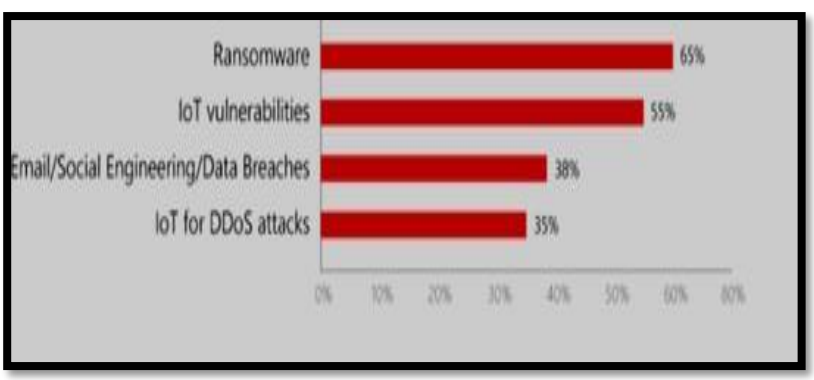

Figure 1: 2017 Top Cyber Security Threats

So, the threats to user's sensitive data and insecure mechanisms of hacking information in the business world urge the demand of preventive cautions and actions against cyber crime.

new security techniques along with its devastating types by all means.

2. TYPES OF CYBER ATTACKS THAT WE NEED TO AVOID FOR OUR BUSINESSES

2016 may be considered as the success of cyber criminals as several serious cyber threats were being faced by the people and the companies. Hackers gain access to their personal information for their own benefits. Despite of these major threats to organization in the past year, 2017 and in its ongoing years are still suspected to get along with these cyber-attacks especially business companies if they do not take any precautions.

2.1 *Sql Injection*

SQL Injection (SQLi) refers to an injection attack where an attacker will render malicious SQL statements through which Relational Database Management System (RDMS) can be controlled any website or web application in which SQL-based database is used probably would be affected by SQL injection using advantage of its vulnerability. It is stated that this can be used by an attacker to bypass authorizations mechanism and web application's authentication. This further leads to get access to the contents of an entire database ultimately threatening main web application. Database records can be added, modified and deleted by using SQL injection[2].

Once control to the database is fetched an attacker is able to have unauthorized access to user's private information through SQL injection. This data can include personally identifiable information (PII), intellectual property, trade secrets, customer belonging details and other sensitive data.

The essentials necessary for an attacker to attack an SQLIA (Structured Query Language Injection Attack) are a web browser, clever guesses of significant tables and field names having an understanding of SQL queries. URLs and user inputs are two approaches through which SQLIAs can be executed. The process for launching such an attack includes four steps. The first step ensures the identification of whether the action is susceptible to a SQLIA. This is attained by finding out if special characters are accepted as input. The conviction of particular kind of database being used by the net application is the next step of releasing a SQLIA.

Different database management systems have variable injection processes so it is beneficial to establish database type. The third step is to collect all the possible information about the database. This step is determined by the attacker's capacity to guess field names, table properties and procedures already stored in the database. The finishing step is to install the attack, currently simple because all of the reconnaissance has already been done by the attacker[3].

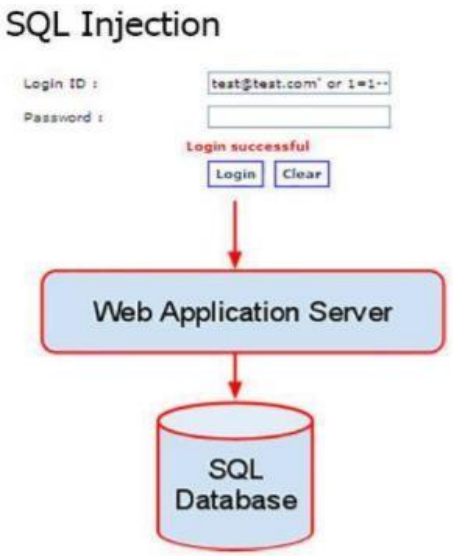

Figure 2: Flow of SQL Injection

2.2. MITM

In computer security and cryptography, there is an attack known as a **man-in-the-middle attack** (**MITM**) in which the hacker or cybercriminal probably changes the transmission mode held between two participants who assume that they are connected to their partner without interference. For instance active eavesdropping; where the offender makes temporary affiliations with the victim and data is transferred between them in a way that they believe they are talking to one another through personal connection, but The attacker by scanning the contents obstruct all related text transmitting within the two sufferers and inculcate new chat. This might be done in many circumstances; for example, an attacker can insert himself as a man-in-the-middle within reception actually the attacker is commanding the whole conversation.

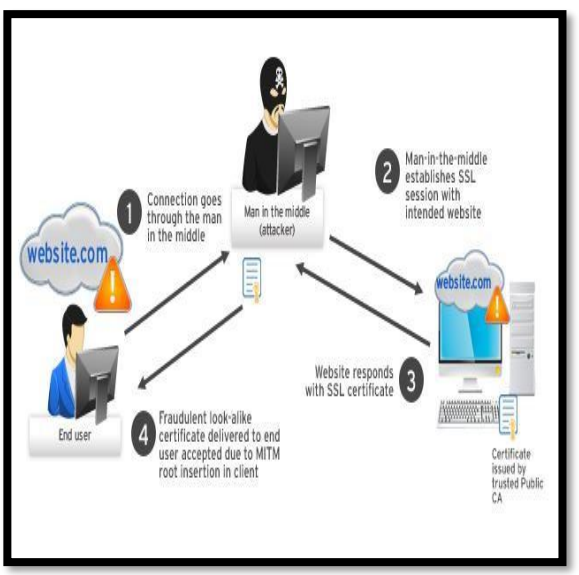

Figure 3: *Man in the middle attack (MITIM)*

range of an unencrypted wireless access points or Wi-Fi's.

Some scientific protocols include various styles of terminating such conversations specifically to stop MITM attacks[4];for instance, TLS (Transport Layer Security) will evidence one or each participant employing a reciprocally trusty certificate authority during this whole process.

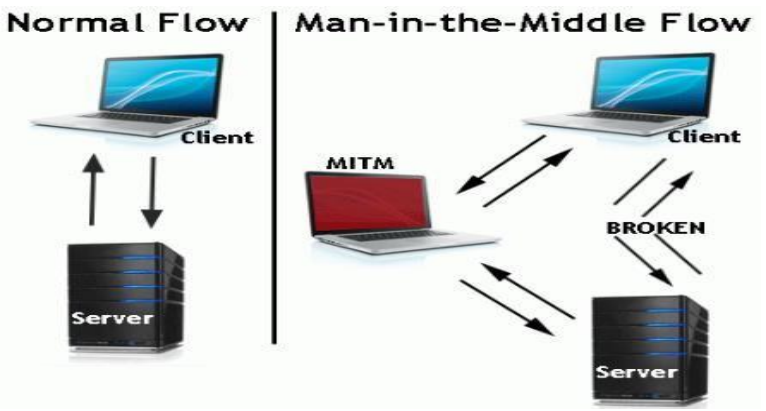

Figure 4: Comparsion of normal flow vs MITM

There occurs a difference of interaction when we talk about a connection of a server and a client and when there is an MITM in between. Direct and indiect communication occur in this regard. This can be seen with the help of fig4.

2.2.1. An illustration of the man-in-the-middle attack:

Suppose Nancy needs to speak with David. Meanwhile, Morgan wants to be a part of this speech to listen in and optionally transfer an untrue text to David. MITM is illustrated below.

a) *Morgan intercepted a message sent by Nancy to David*

Nancy "Hello David, I want your key, Its Nancy." → David known to Morgan

b) *This message is conveyed to Mallory and Bob who are unable to tell whether this is by Nancy.*

Nancy Morgan "Hello David, I want your key, Its Alice." → Bob

c) Bob replies with his encryption key:

Nancy Morgan ← [David's key] David

d) Declaring that it is David's key, Morgan responds to Nancy by changing Bobs key with her own

Nancy ← [Morgan's key] Morgan David

e) Nancy thought solely David will browse it. A message is encoded by Nancy which is assumed by her to be David's key

Alice "Need to see you at the railway stop!" [encoded with Morgan's key] → Morgan David

f) However, it is actually encoded , decoded , read , modified (if desired) by Morgan key, re-encrypt with David's key, and send it to David:

Nancy Morgan "Meet me at the van side by the cafe!" [Encoded with David's key] → David

g) According to David, he is connecting securely to Nancy.
h) Morgan robs identity of David as he goes to the van side by the cafe.

The example indicates the requirement for Bob and Alice to own a way to confirm that each other's public keys are used by them actually, instead of the general public key of an attacker. MITM attacks can be protected by using variable techniques. Two ways largely defend the MITM attacks: these include tamper detection and authentication. Some degree of guarantee about an incoming message from the sender is provided by authentication. Comparatively the means of tamper detection gives the proof.

3. PHISHING

Phishing may be one of the poisoning attacks during which the attacker tries to find out the data like login credentials by faking a reputable person in electronic mail or in IM[5].

Phishing is methodically done by considerable messaging or electronic mail to penetrate concrete data at a site that is

robbed. The messages have connections to various links that enable malware problems. Attempts to govern the development of spoofing occurrences incorporate enactment, dependent preparing and specialized efforts by effective techniques.

3.1. Types of phishing

3.1.1. Spear phishing: The maximum used type of phishing is spear phishing. No, it's no longer a regular task, it is a trick and you are the goal. Spear phishing is an e- mail that offers an influence of being from an individual or enterprise which you know. In any case, it is not, it's from similar crook programmers who need your charge card and ledger numbers, passwords, and the budgetary facts in your PC. The need is to figure out how to ensure safety from this kind of attacks[6].

3.1.1.1. Email from a "Companion": Phishing prospers with recognition. He is aware of your call, your e-mail address, and no less than a bit approximately you. The welcome on the email message is probably going to be customized: "Hello there Bob" as opposed to "Dear Sir." The electronic mail may additionally make reference to a "shared companion". Since the e-mail seems to originate from any person you understand, this increases when you are probably less cautious and provide them the facts they request.

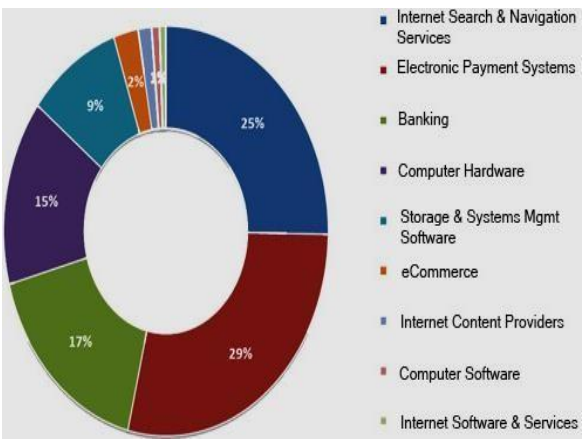

Figure 5: Percentage description of Phishing Attacks

3.1.1.2. Utilizing your web presence against you: How could you switch into a goal of a lance phisher? More likely, from the information you put on the Internet out of your PC or mobile phone. For instance, they may take a look at casual conversation locations, find out your page, your e-mails, cope with your companions list and might

start an attack with the aid of your enlightening partners to procure at a retail webpage. Utilizing those facts, a lance

logo for your picture web page. They will look for that keyword and try to get to your file on that online retail internet site you use. Alternatively the lance phisher can also utilize indistinguishable information from the play store and request to reset your secret key, or re-affirm your Visa range. This ultimately can lead to financial crisis.

phisher ought to act like a companion, ship you an electronic mail, and illustrates a procedure.

3.2. Clone Phishing: A sort of phishing assault that can spread through an email by establishing a connection that can inculcate various addresses for sending an identical email.

3.3. Whaling: These kinds of attacks are coordinated at major concerns like respectable officials and can be a threat for people inside the organizations to affect their working[7].

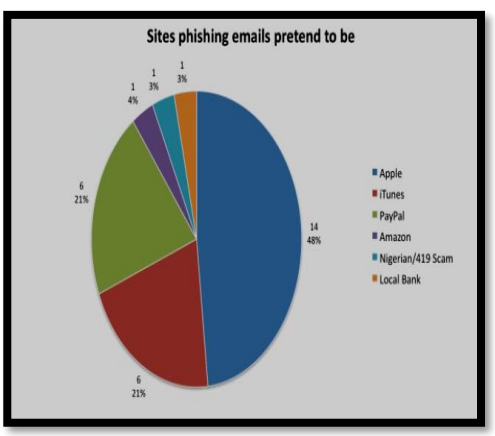

Figure 6: Various Phishing Emails

3.4. Avoidance technique from phishing:

There is a remedy that gives help in encounter spoofing. The Anti-Phishing Working Group Inc. also the middle regulation's OnGuardOnline.gov gives scheme on this increasing cyber crime to

refrain from spoofing charge. Intelligent load serve, for example, Wombat Security Technologies' Anti-Phishing Training Suite or PhishMe can relieve the representatives how to abandon from spoofing problems, while FraudWatch International and MillerSmiles administer the most neoteric

spoofing mails ownership that spreads through the Internet.

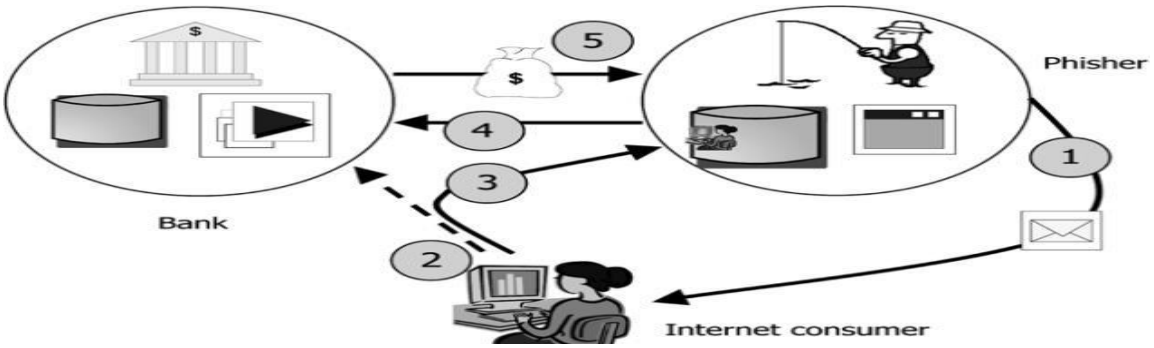

Figure 7: Symbolic Flow of Phishing

4. ROGUE SOFTWARE

Rogue security software is a form of malignant programming and web extortion that deludes clients to accept that there is a harmful attack on their PC, and controls them into paying cash for a fake malware evacuation device (that really acquaints malware with the PC). It is a type of product that controls clients through dread, and is a type of payment product. Maverick security programming has turned into a genuine security danger in desktop figuring since 2008.

4.1. Working*:* A site may show a fake cautionary message expressing that somebody's machine comprises of a PC infection, and urge them through control to introduce or buy this product with the confirmation that they are obtaining certifiable antivirus programmed software. The programmers more often attempt to make the clients trust that introducing the security software's is not always their last choice. The strategy is, not to follow everything that shows up on your PC. Counteractive action: The main answer for the issue is to utilize presence of mind and never get stuck in such circumstances. Additionally, the framework of software ought to be kept up-to-data[8].

5. MALWARE: Malware is stated as a kind of programming that can silently get to a tool without the clients notice. Web with the aid of techniques for e-mail, malwares can get approach to the system through hacked destinations, entertainment history, track data, toolbars, corrupted software, free participations, anything else you download from the web onto a device which is not always secured in opposition to malware programming. You can use a malware scanner to check if your tool is infected. The best technique to get rid of malware is to cope with discarded malwares as observed in any first-rate

antagonistic to malware programming e.g. Avast Free Antivirus.

***5.1. Steps to prevent from malware*:** Use updated antivirus software's to detect malware attacks. There is no other manner to cope with malware than to use an antivirus and antagonistic to malware infected machine.

6. RECONNAISSANCE: In military operations, observation is the investigation outside a region involved by amicable powers to pick up data about characteristic components and adversary nearness. Cases of surveillance incorporate watching by troops, ships or submarines, satellites, or by setting up disguised perception posts. Since observation is military's exceptional strengths working in front of its fundamental powers; spies are non-warriors working behind adversary lines. There are two sorts of observation assaults:

- Active
- Passive

Latest observational attacks are the point at which an attacker searches for private data without drawing in with the casualty's frameworks**.** The two types occur once in a while where reconnaissance is obtained from its utilization in military varying from the dynamic assaults[9].

6.1. Working and prevention: In a PC security measures is for the most part a preliminary step towards stopping a future attack. The attacker often possibly uses port addresses to locate any feeble ports. After a port scope is revealed the vulnerabilities of organizations related with open ports are perceived. For remedial action the slightest complex way to deal with suspect most port or to yield attacks or reconnaissance strikes is to use an Intrusion Prevention System and add firewall. The firewall controls the ports which are displayed to whom they are exhibited. The IPS can perceive port outcomes in time and close them down before the attacker can get a full guide of your framework.

7. SSL ATTACKS: Secure Sockets Layer (SSL) is a PC networking protocol for securing associations between an organized application of customers and servers over an unreliable system like the web. Because of various conventions SSL was expostulated for use on the web by the Internet Engineering Task Force (IETF) in 2015 and has been supplanted by the Transport Layer Security (TLS) convention[10].SSL keeps running over the network layer and the transport layer, which are in charge of the vehicle of information amongst forms and the directing of system movement over a system amongst customer and server and underneath application layer, for example, HTTP and the Simple Mail Transport Protocol[11].

7.1.Working: An SSL assault type blocks the scrambled information before it may be encoded, enabling the assailant to approach to sensitive information including Visa

8. DENIAL OF SERVICE

In Denial of service: (DoS), a mastermind seeks a chance of making a network resource unavailable through some temporary settings. It is a cyber-attack that can affect a machine targeting some intended users by disrupting the services of a host connected by means of a network. It works by over flooding the machine with so many requests at a time that its gets in a halt state or in such a position that no important requests of the users are satisfied.

Some of the important defensive measures in this regard include IPS based prevention, Firewalls, router and switches for rate limiting and traffic shaping and upstream filtering[12].

9. DRIVE BY DOWNLOADS:A drive-by download is a program that is consequently downloaded to your PC without your assent or even your insight. Not at all like a pop up download, which requests consent (but in a figured way prone to prompt a "yes"), a drive-by download can be started by just going by a Web website or review a HTML email message. In the event that your PC's security settings are not up to the mark, it might be workable for drive-by downloads to happen with no further activity on your parts[13].

10. MALVERTISING: Malvertising is the utilization of web based publicizing to spread malware. Malvertising includes infusing malignant or malware-loaded commercials into true blue web based promoting systems and web pages[9].

Publicizing substance can be embedded into prominent and respectable sites, malvertising give cyber criminals a chance to push their attacks to web clients who may not generally observe the advertisements, because of firewalls. Malvertising is appealing to assailants since they 'can be effortlessly spread over a substantial number of sites without specifically trading off those websites'. Malvertising is a genuinely new idea for spreading malware and is much harder to battle since it can work its way into a site page and spread through a framework unconsciously. Attackers have a wide reach and they can convey these assaults effectively through commercial systems. Organizations and sites have experienced issues decreasing the quantity of malvertising assaults, which "recommends that this attacking vector is not probably going to vanish soon[14].

***10.1. Working and prevention*:** Sites or web distributers accidentally consolidate a vindictive notice into their page. PCs can end up noticeably infected by a pre-snap and post click. It is a misguided judgment that problem just happens when users start tapping on a malvertisement.

Malware can likewise auto-keep running, as on account of auto diverts, where the client is naturally taken to an alternate site, which could be noxious. To keep malvertising from tainting your PC, you have to deny misuse units the chance to discover a defect. Spieled encouraged individuals to ensure their Web programs and program modules, (for example, Java or Adobe Flash), and additionally working frameworks, to be updated with the goal that known harms are settled.

11. PROTECTION OF DATA FROM CYBER ATTACKS

To ensure a very secure and strong password. If you find a self-assertive USB stick, do not allow yourself to associate it to the remote possibility that you do not place stock in the source, you're in a perfect circumstance not putting your PC at shot. Keep away from embeddings hard drives and thumb drives you do not trust into your PC. Guarantee a site is secure before you enter particular information.

In case these things are not there, by then the framework is not secure and you shouldn't enter any information you wouldn't require. Sending essential information, for instance, Visa numbers or money related numbers puts it at risk of being hacked by software engineers or computerized strikes. When in doubt, a software engineer will use this email or site to present noxious programming onto your PC. These web components are planned to look like a common email or website, which is the way developers convince people to hand over individual information[15].

12. CONCLUSION

Through this research it is clear that there is a need to take care of the issue talked about at the outset and to protect ourselves from these malicious kinds of attacks by first and fore mostly having updated antivirus software installed. If any kind of pop up or harmful message is shown up on the screen client ought to never fears or get panic and do whatever the pop up is asking on the grounds as these are tricks utilized by programmers to inculcate user's interest and get his/her system's control. In addition clients need to never set those passwords which are too easy to hack. Solid passwords ought to be connected, users needs to dependably utilize latest firewalls to remain safe and never tap on advertisements or connections which they do not have any assure idea. This overview on emerging cyber-attacks in the business world along with their working and preventions opens doors for researchers to study on categories of malwares, network security measures, engineering and programming techniques using firewalls to overcome the rapid growth of attacks in all aspects.

13. REFERENCES

[1] Lavanya, M., & Sahoo, P. K. (2016).IP spoofing and its Detection Technique. IJACTA, 4(1), 167-169.

[2] Panah, M. V., Bayat, N. K., Asami, A., & Shahmirzadi, M. A. (2016). SQL Injection Attacks: A Systematic Review. International Journal of Computer Science and Information Security, 14(12), 678.

[3] Mavromoustakos, S., Patel, A., Chaudhary, K., Chokshi, P., & Patel, S. (2016, December). Causes and Prevention of SQL Injection Attacks in Web Applications. In Proceedings of the 4th International Conference on Information and Network Security (pp. 55-59). ACM**.**

[4] Arshad, M., &Hussain, M. A. (2016). Secure Framework to Mitigate Man-in-the-Middle Attack over SSL Protocol. Indian Journal of Science and Technology, 9(47**).**

[5] Ekawade, S., Mule, S., &Patkar, U. (2016). Phishing Attacks and Its Preventions. Imperial Journal of Interdisciplinary Research, 2(12).

[6] Zhao, M., An, B., &Kiekintveld, C. (2016, February). Optimizing Personalized Email Filtering Thresholds to Mitigate Sequential Spear Phishing Attacks. In AAAI (pp. 658-665).

[7] Heartfield, R., &Loukas, G. (2016), A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 37

[8]**.** England, P., Slick, G., Dunn, J. C., Ray, K. D., Peinado, M., &Willman, B. (2016). U.S. Patent Application No. 15/047,300.

[9] Pathak, P. B. (2016). Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. International Journal of Advanced Research in Computer Science, 7(2).

[10] Nguyen, H. T., &Dinh, T. N. (2016, April). Targeted cyber-attacks: Unveiling target reconnaissance strategy via Social Networks. In Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on (pp. 288-293).

[11]**.** IEEE. Sirohi, P., Agarwal, A., &Tyagi, S. (2016, October). A comprehensive study on security attacks on SSL/TLS protocol. In Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on (pp. 893-898). IEEE.

[12] Tarao, M., & Okamoto, T. (2016). Toward an Artificial Immune Server against Cyber Attacks: Enhancement of Protection against DoS Attacks. Procedia Computer Science, 96, 1137-1146.

[13] Sood, A. K., &Zeadally, S. (2016). Drive-By Download Attacks: A Comparative Study. IT Professional, 18(5), 18-25.

[14] Pathak, P. B. (2016), Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. International Journal of Advanced Research in Computer Science, 7(2).

[15] Lee, N. (2015). Cyber-attacks, prevention, and countermeasures. In Counterterrorism and Cybersecurity (pp. 249-286). Springer International Publishing.