# A Systematic Review of Cyber Security and Classification of Attacks in Networks

Muhammad Kashif[1], Sheraz Arshad Malik[2], Muhammad Tahir Abdullah[3], Muhammad Umair[4]
Department of Information technology,
GC University,
Faisalabad, Pakistan

Prince Waqas Khan[5]
Department of Computer Science,
University of Agriculture,
Faisalabad, Pakistan

***Abstract*—Cyber security plays an important role to secure the people who use internet via different electronic devices in their daily life. Some causes occurred all over world that people face problems when they connect their devices and system via internet. There are some highly sensitive data like biotechnology and military assets which are highly threatened by the hackers; cyber security plays a vital role in securing such data. Misusing the internet becomes a current issue in different sectors of life especially in social media, universities and government organizations. Internet is very useful for students in study institutes and employees who work in different organizations. Internet source gives the facility to people to fetch some information via internet. However, they must be protected when use the internet and secure for any unauthorized access. In this paper we have covered the different aspect of cyber security and Network security in the modern era. We have also tried to cover the threats in Intranet of organizations.**

***Keywords*—Cyber security; internet; intranet; network security; cybercrime and security alludes***

## I. INTRODUCTION

During the last decade, access to information technology (ICT) has surged across the world. Broadband technology is now available to billions more it was just years in the past. The access of computer internet technology has large benefits but on the other hand there are several issues to reaping these benefits. Among all those challenges one of the biggest challenge is cyber security. In any computer network environment successful security infrastructure must meet the three basics objectives that are CIA (confidential integrity, availability) without obtaining the goals of these requirements it's not feasible to achieve the goal of secure internet. Against a setting of the Internet of Things-based DDoS assaults researchers come to know that in the recent years, it is termed as "death of the internet". Now it is very easy for someone who wants to turn down the internet. They will start attacking the service provides [1]. In this paper we have discuss different type of Security attacks which can affect internet. Here we discuss about the major attacks of daily routine which are the reason of security breach. We can also mention the counter measure how we can secure our Internet from those attacks Internet security is one of the biggest challenge of computer era as we know that internet is also provided Internet As A Services (IAAS). Security is becoming challenge for both internet consumers and internet provider computer networks are part of our daily life their security as important as on the off chance that we have a learning of different web assaults as we can shield yourself from these assaults. Purpose of implementing CIA triad is to make internet secure and the whole network. The purpose of this model is to save from damage of internet security and to stop misuse of data. There are many ability pitfalls which could stand up if network protection isn't implemented well.

Internet is a telecommunications network that use guided and unguided media (phone lines, satellites, and links) to associate PCs and different gadgets to the internet. All PCs, mobiles, TV, and diverse electronic gadgets can associate with the Internet. Internet is becoming an important source for people of world who use in different kinds of work in their daily life. The graph of using internet in all over world including developed and developing countries has increasing day by day. The latest technologies are also introducing with passage of time the people's requirement related to internet and fast access of any thing is also increase. Web was utilized as a part of military, guard working activities, and for one of a kind college's examination purposes. Presently in this century it has developed in all sectors of life including information, business, social life, education, entertainment, data sharing service, and shopping. There are many advantages and disadvantages. In disadvantages of internet is online fraud, cyber terrorism, identity theft, and other cybercrimes are mostly commit by any unauthorized third party. This reason cyber security is very important for users of internet and they feel protected when they will use internet [2]. Cyber security gives the assurance and guarantees to internet users their communication way/internet is secure and protected against any attack of unauthorized third person.

## II. CYBER SECURITY

Cyber security is the set of rules, body of technologies, processes and procedures to protect the electronic data, networks, computers, and programs from any attack and unauthorized access. Cyber security must satisfy three points:

*1)* Measure amount of data for the protection of information technology.

*2)* The Level of protection as an outcome from application of those taken measures.

*3)* The field associated with the professional endeavor.

These three aspects of cyber security play a vital role to prevent and secure a personal data of every user of internet, business, and government [3]. Those data are essential because they can be hacked by other person for illegal activities. Various powers oversee the lofty ascent in hostile cyber intrusions and unapproved network breaks. The blast of new advancements and development of societal reliance on all-inclusive interconnected innovation, joined with the robotization and commoditization of cyberattack tools, digital aggressor modernity, and low passage hindrances into the cybercrime market 10 are no uncertainty among the key ones [4].

## III. Digital Security Alludes

The significance of cyber security tends to be chosen in various settings. At times, it alludes to monetary terms or in social and social terms or even in politics and military terms. As it is regularly utilized, “digital security” alludes to 3 (three) things:

*1)* A course of action of activities and diverse measures wanted to guarantee from strike, intrusion, or distinctive risks PCs and unique segments of the web.

*2)* The state or nature of being protected from such risks. The activities can join security surveys, settle organization, approval systems, get to organization, and so on.

*3)* The extensive field of take a stab at, including investigation and examination, went for realizing and improving those activities and quality [3].

Web client is developing significantly in assortment age and the motivation behind utilizing web at that point is done in different courses as clarified previously. They can incorporate, such as, investigate and estimate the feature and susceptibility of the gear and programming used as a piece of the country's political and money related electronic structure. They furthermore incorporate revelation and response to safety occasion, lightening of impacts, and repossession of pretentious portions. Diverse compute can join such things as gear and programming hardware & software firewalls, physically protection, for instance, cemented workplaces, and personnel getting ready and commitments. The quantity of web clients in Indonesia for instance is expanding each year. As indicated by Internet [5] business web administrations started in Bahasa Indonesia at 1995 and imminent in 2008, Malay had a normally more than 25 million Internet users. It is foreseen that in starting of 2013, the amount of web users in Indonesian is getting the chance to be observably more noteworthy than in 2008. [6] also communicates that web customers in Indonesia is scramble definitely finished the latest two calendar years, “20 ratio of Indonesians 14 at another time and more settled now get to the Internet reliably. That is more than million people and growing reliably consistently. Regardless, we need to review two fundamental facts that depict the utilization. In the first place, around ten of the thirty million customers get to the Internet by methods for their cell phones. Secondly, around 70 ratios of those 30 million customers visit web Facebook, YouTube and twitter every month, creating in the most predominant location in the country” [7]. This reality truly isn't amazing considering the way that PC and its ability containing web as preface has been displayed since the adolescents in review school. It infers that the Indonesian youngsters particularly college understudies have expertise to get to web yet they are additionally possibly to abuse or to be abused by the web. Nearness of web for understudies in college really encourages them to get a considerable measure of data identified with their assignments. The data is given in types of book on the web and diaries. The two books and diaries give a simple assignment for the understudies to complete their undertakings specific when they lead their last paper to be graduated. In any case, a great deal of instances of abuse the web work additionally led by college understudies. Counterfeiting is a standout amongst the most web abuse led by the understudies. They tend to duplicate a few materials to their undertakings however they don't say the creator's name. Other web abuse can be discovered, for example, unlawful substance, online extortion, and wholesale fraud.

### *A. Classes of Strike*

As indicated by National Research Council in the year 2003, there are 3 (three) classes of strike that directed to web, as following:

*1) Organization unsettling influence*: It causes lost organization and can come to fruition because of debilitating of frameworks through a grouping of attacks, for instance, repudiation of organization (DoS) and pummeling of information [8].

*2) Theft of favorable circumstances*: It mainly handles essential information on an adequately immense scale to have genuine impact.

*3) Catch and control*: It’s incorporates catching all controls of the web and apply this as an armament. These levels of strike or attacks are label as a cyber-crime and moreover have been balanced in various manners. That modus in certainty undermine every single individual exercise including framework.

### *B. Dealing with the Violations*

To deal with and to keep those violations, digital security assumes vital part to ensure individuals to utilize web securely. As we known, the internet aggregates a gigantic scope of related components of the internet exercises and it is in this way the internet exercises are conceivably in danger. To take out or expel the hazard, insurance of the internet framework is required keeping in mind the end goal to stop programmers to perpetrate their violations. The assurance of the foundation must cover web equipment, media communications framework, processing gadgets as control framework and figuring gadgets as personal computer [9] moreover stipulates that to take out the hazard isn't just security to the foundation (equipment) yet in addition must ensure the product. Insurance of programming is proposed to help everyone to utilize PC/web securely. It is because such many PCs are utilized as a part of homes and organizations. The PC working frameworks and email programs are two parts of PC/web that is powerless against be assaulted and misused. Instance of PC worms that smacked MS Windows working structure in 2003 was a evidence to see that the prevention of write the computer programs is relied upon to guarantee the web customer; or other case of a worm happened in 2010, when a worm called Stuxnet was impelled to strike the Iran nuclear power plant agenda. [10].

Both protection of gear and writing computer programs are the essential reason for advanced security. They can surety people to use web soundly and safely. People will use web to help their activities with no agonize too pessimistic for impact of web. Regardless, the two preservations must be executed and introduced in domestic and widespread master plan or policy (control) to accomplish its targets. In United States, e.g., it can be found National Strategic plan for motherland protection. The inspirations driving this system are to check computerized ambushes against fundamental structure; to reduce domestic vulnerableness to advanced attack; and, to restrain the mischief and regaining duration from computerized attacks that do happen or another case in Canada, it’s domestic procedure is determined to 3 segments: protecting governing body of a nation structures; working together with the privately owned fragment; and serving its citizens to  protect connected through care boost and raising [3].

Internet misuse is mostly committed by the younger generation their ages between 16 to 22 years. They are all belongs to different study’s institutes. They are use internet for financial fraud. These types of people hacked the other people accounts, ATM card PIN numbers, and important data. Social media is also a major and critical platform whose misuse by many illegal persons. The cyber terrorism activities are also occurred via this source in all over country. The misusers post the unethical posts on Facebook, WhatsApp, and Twitter, etc. For harmed the people. In forecast countries e.g., Indonesia, etc. has a law against cybercrimes but in Pakistan there is no any law against cybercrime introduced or implemented in country. That’s why the misuse of internet is increase day by day all over country. If any Law implemented in all over country against these kinds of people and Pakistan telecommunication authority, other agencies monitor the all activities and communication with help of cyber security techniques. Then we will overcome on this problem in very few time of period.

## IV. Intranet and Multilevel Security Management

Many organizations are moving toward a private internet or personalized source of internet within the organization mostly called intranet. Intranet is an inside a vital piece of information system based on Internet knowledge, TCP/IP, HTTP transmission rules and website services. The intranet is an innovation that enables your association to characterize itself all in all element, a gathering and a family, where everybody knows their parts and everybody is chipping away at the change of the association.

As on the Internet, there will be specific goals and information and data on the intranet that ought to be kept puzzle from work drive, e.g. fund and helpful information. Measures are hence vital to ensure that these advantages are used and gotten to in a secured and orderly form. In a circumstance where there are just two sorts of assembled information, e.g. 'portrayed' and 'unclassified', access to these different sorts of information can be controlled by strategies for an ordinary access control procedure, e.g. a mystery word. If you know the mystery word, you will get to the more unstable information. Else, you may be allowed to see the non-sensitive information. Associations differentiate nevertheless, and military and government circumstances make the protected securing of information living on these intranets fundamentally more troublesome. The clarification behind this is the request of information as showed by its substance [11]. Out of the blue there aren't just two specific requests of data any more, however in the military condition for example, there are more game plans, i.e. Constrained, Classified, Secret and Top Secret. The number of groupings of data is settled only by the earth and can be practically than in the already said representation.

An intranet could comprise of a WAN (Wide Area Network) with many LAN (Local Area Networks) associated with it. Each of these LAN's alone can bolster an expansive number of workstations, servers, work area PC's, fringe gadgets and so on. Every one of these contraptions related with the intranet could have a security gathering. Heartbreakingly it's not just the devices that have a security gathering, yet the information they store or process as well. Every one of the information on a LAN can have the same or unmistakable arrangements. These elements befuddle security matters truly. Work power will in like manner have plans which will allow them access to information with orders equal or lower than their own specific gathering. This oversee is gotten from the Bell-Lapadula Model which is a famous security model. Clearly indicates for a relationship to empower most of its work power to use such an intranet direct is a critical troublesome task. If an affiliation is made to the web as well, the issue ends up being altogether more troublesome. Clearly the extended number of requests - i.e. Multi-Level Security - of data makes a charming issue in respects security in an intranet space. The change of modern and advanced Internet of Things has pulled in an impressive measure of enthusiasm from different research schools. The recognizing verification of people and things has permitted their portrayal in a propelled world through radio frequency distinguishing proof developments. This has enabled numerous applications to be delivered for key traceability and aerating and access control in various zones, for instance, transportation, mechanical or building [12].

## V. Advances of Overseeing Multilevel Security

There are a few advances are utilized for overseeing multilevel security in military condition.

### *A. Onion Routing*

Onion routing is a technique for unusual correspondence on a computer network. In an onion network, messages are summarized in coatings of encoding, closely resembling layers of an onion [13]. This scrambled information is communicated through a progression of system hubs also called onion switches, every one of which "peels" left an unsociable layer, revealing the information's next target. At the point when the past layer is decoded, the message lands at its target. The source stays unknown because every delegate identifies just the area of the promptly going before and following hubs.

### *B. Intelligent Agents*

A keen specialist is an item that enables people and take after to up for their purpose. Savvy administrator's effort by empowering persons to name work that they could have finished, to the pro programming. Pros can accomplish dull errands, remember things you disregarded, keenly diagram complicated information, pick up from you and even influence proposal to you. To see how clever operators function, it is best to inspect a portion of the down to earth issues that shrewd specialist can help comprehend. A canny specialist can enable you to discover and channel info when you are viewing data or browsing the Internet and don't recognize where the correct information is. It could likewise re-try information to your slants, consequently save you time of dealing with it as additional latest information arrived every day on the Internet.

## VI. Requirements for Network Security

Network security is the procedure through which we can ensure the computerized data. It is so urgent for all systems must be shielded from dangers and the dangers with the goal that a business can accomplish its fullest potential. With the advances in microelectronics, embedded processing, and wireless communications, the enthusiasm for Body Sensor Networks has risen pointedly and has empowered the improvement and usage of such systems There are no models or rules on estimating a scheme`s productivity. Security investigation is infrequently performed with formal strategies; rather, spellbinding examination is typical [14]. The target of system security is

*1)* To secure the secrecy the data must be gotten to and examined just by the endorsed individuals or social occasions. It is the protection of the individual information. We can differentiate order and security. Data encryption, User Ids and passwords, bio metric checks are a bit of the methodologies through which characterization can be secured.

*2)* To keep up Integrity it is the affirmation of not only the information can be gotten to or changes by the endorsed individuals presently moreover the data must be exact, unfaltering completed on the off chance that it can recall cycle. Measures taken to ensure respectability consolidate controlling the physical state of sorted out servers, limited access to data, and develop intensive check practices. Cryptography expect a to a great degree genuine part in ensuring the data uprightness. Hashing the data, you get and differentiating it and the hash of extraordinary message is another system to ensure data uprightness.

*3)* To ensure that the Availability of Data must be open to the endorsed individuals at the perfect time. It can be ensured by completely keeping up all hardware, preparing gear repairs rapidly and keeping up an adequately working system condition. Standard fortification must be taken, for information benefits that are exceedingly essential, abundance is fitting procedure to ensure availability.

## VII. Complications in Network Security

Major Cyber Attacks and their counter measure as internet is facing number of security problems. That is the job of the network security to keep the system ensure against malevolent programming, worms, and dangers and different assaults. An assault is a data security risk through which the social criminal endeavor to get past, change, evacuate, embed or screen essential data without approved get right of section or consents.

### *A. Malware*

Malware is a truncated term implying "malevolent programming". This is programming that is especially expected to get passageway or mischief a PC. Unmistakable sorts of malware are spyware, key loggers, honest to goodness contaminations, worms, or any sort of malignant code that mischief a PC. Overall, writing computer programs is recognizing malware in perspective of the desire of the creator as contradicted to its real highlights. Prior to the term malware was begat by [15], malignant programming was alluded to as PC infections. Malware is habitually familiar with a machine through email associations, programming program downloads or working structure vulnerabilities.

*1) Counter measure for malware*: The most ideal path against malware is to stop downloading contents from the untrusted internet sources and users just try to improve security. That is now and again accomplished through deploying strong and up to date firewalls, which prevent the unwanted traffic and it allows only the rusted traffic. While applying the different access control lists. It allows you to segregate the desired IP addresses which you want to allow in your Network. It must be checked out after rapid interval that operating system (for example Ubuntu, Windows, Mac OS X, centos and Linux) you use has the most updated security policy. Software developers update their software frequently to overcome the weak points for this purpose one should use up to date version of software. For example, the OS corporations like Microsoft, launch the updates for their OS often.

### *B. Phishing*

Much of the time acting like an interest in data from a put stock in pariah, phishing attacks are sent by methods for email and demand that customers tap on an association and enter their own data. Phishing messages have turned out to be fundamentally more refined recently, making it troublesome for a couple of individuals to perceive a real interest for information from a false one. Phishing messages as often as possible fall into an undefined grouping from spam. yet are more destructive than only a straightforward promotion.

Research done by indicated that users effectively identified just 53% of phishing sites notwithstanding when prepared to recognize them and that they for the most part invest almost no energy looking at security markers contrasted with site content when making appraisals [16].

Phishing messages consolidate an association that aides the customer to a false site that will take a customer's information. From time to time, every one of a client desires to do is tap on the association. For example, in the past few years social media are the main and easy target of Pashing. Hackers create a fake page for social media site and the Victim think that it is original site, so he provides the credentials and get hacked easily Check any requirements from associations that touch base by means of email via telephone. If the email itself has a telephone number, don't call that number, however rather one you find unreservedly on the web or inside documentation you've gotten from that organization. User must check the URL of the accessing website before entering their credentials. The protocol must be checked that it is HTTP or HTTPS, HTTPS is more secure to give the personal information. Many companies warn users not to give any personal information over the Email or Telephone without verification. So, a user must double check before providing his sensitive information over the web.

### *C. Attacks on System via Password*

The password is the most sensitive information a user could have over the internet. But most of the times user use the easy and simple words as their password which are easy to remember for him. For example, 1234, his mobile number, Birthdate, his own name or country name. Sometimes user set the same username and password for his convenience. The hacker tries to break your password using your public information.

This does not require any special algorithm or programming technique. It works just by entering Words which user could use as password.

To avert this, a user must use the complex password. His password must be at least 8 charters long. It should contain upper case, lower case letters, numbers and special characters. User should avoid using his personal pubic information like his own name as password. Do not use the words available in the dictionary. Password must be changes frequently.

### *D. Attacks on System via Denial-of-Service (DoS)*

A DoS assault centers around entering the excessive information to break the security. To slow down the performance of a server or in some cases completely down the services, the hacker sends the fake requests in a large number of amount.

There are two or three different ways aggressors can achieve DoS assaults, however the most widely recognized is the circulated dissent of-advantage (DDoS) assault. This includes installing a third-party software to send the large number of fake requests to access the server. Due to this server stop to respond to the real or actual requests.

Using the advance level firewall could help to protect your system from such attacks. If a MAC address is broadcasting enormous number of requests in small time intelligent firewall will automatically block that traffic. Unless your association is massive, it's uncommon that you would be focused by an outside collecting or attacker for a DoS attack. Your site or system could even now surrender to one, be that as it may, if one more association on your organization is focused on. The most perfect method to keep an extra rupture is to keep your framework as secure as possible with normal program writing energizes, online safety detecting and examination your information stream to identify any bizarre or incapacitating points in rush hour jam before they turn into a problem. DoS attacks can similarly be performed by fundamentally cutting a link or removing a fitting that interfaces your site's server to the web, so due persistence in physically detecting your associations is suggested too. Simply cutting a cable or dislodging a plug that connects your website’s server to the internet, so due assiduousness in physically monitoring your networks is suggested as well.

### *E. “MAN in the Mid” (MITM)*

By copying the endpoints in an online data exchange (For example the connection from your mobile phone to a web site) the MITM can gain your info from the end client and the module he or she is talking with. For occurrence, in case you are spending money on the different website, the man in the inside would conversation with you by impersonating your bank, and talk with the bank by rivalling you. The man in the inside would then get most of the info traded between the two gatherings, which could incorporate sensitive information, for example, financial balances and specific individual data.

Often, a MITM gains entry over a non-encoded remote entree point (For example one that doesn't utilize WAP, WPA, WPA2 or other protection efforts). They would then move toward most of the information being swaped among the two gatherings.

The greatest perfect method to counter them is to just apply encoded remote access attentions that Applying WPA & WPA2 safety or more prominent. On the off casual that you must interface with a site, ensure it uses a HTTPS association or, for excellent or effective security, consider inserting resources into a VPN (virtual private network). HTTPS uses validations that check the identity of the server machine you're interfacing with using an outsider association, for occurrence, VeriSign, while VPN (Virtual private network) allow you to link with areas through virtual private network.

### *F. Drive-By Downloads*

Through malware on a true-blue site, a program is downloaded to a client's structure just by passing by the site. It doesn't need any type of motion by the customer to download.

Generally, a little part of code is downloaded to the client's outline and that code at that point links with one more PC to get the rest and download the package. It frequently manipulates vulnerabilities in the customer's working framework or in various plans, for example, Adobe and Java.

The most perfect path is to make certain the bigger portion of your working systems and programming agendas are flow of blood edge. This cuts down your danger of inadequacy. Furthermore, try to confine the amount of program additional things you use as these can be viably replaced off. For example, if your PCs needn't waste time with Flash or the Java component, consider uninstalling them.

### G. Malvertising

A method to job off your PC with malicious code is downloaded to your outline when you tap on a partial announcement. Malvertising strategies are tormenting the web promoting business—offenders are procuring benefits by posting authentic commercials at content robbery destinations or utilizing a multitude of botnets to counterfeit publicizing movement [17].

Computerized aggressors exchange debased show advancements to different targets using an ad compose. These commercials are then passed on to goals that match definite amount watchwords and chase specification. Once a client taps on one of those advertisements, malware will have downloaded. Any webpage or web provider can be put through to malvertising, and several don't know they've been exchanged off.

The best way to deal with thwart surrendering to Malvern is to use sound to decide. Any improvement that confirms resources, free PCs or goes to the Bahamas is likely pipe dream, and thusly could be disguising malware. Of course, in the current style programmed and working structures are your best first line of protection.

### H. Rogue Software

Malware that pretenses as genuine and essential safety programming will protect your framework.

Revolutionary safety programming fashioners make fly up windows and alerts that saw true blue. These alerts urge the customer to download safety programming, agree to terms or revive their existing system with an eventual objective to remain sure. By clicking "yes" to any of these conditions, the dissident writing computer programs is downloaded to the customer's PC.

The best protection is an average offense—for this circumstance, a revived firewall. Guarantee you have a working single in your workplace that protections you and your agents from these categories of attacks. It is also a savvy assumed to acquaint a put stock in antagonistic with contamination or against spyware programming program that can identify threat like free intellectual programming. Similarly, as with furthermost categories of bad actions, circumspection is one of the way to revolution. As computerized stranger ends up being more advanced and more trades relocate on the web, the quantity of risks to persons and federation will carry on developing. Prepare by own and its own trade put separately the chance to protect own systems and made computerized security a need. If you appreciate about some exceptional ways to agreement with keep on wary opposed computerized attacks, it's continuously best to start at home. At this time are eight methods to guarantee your organization's data is protected.

## VIII. Conclusion

Internet has become a basic part of life in all over world. There are many advantages and disadvantages. The critical advantage is misuse of internet by criminal persons via unauthorized access and sources. People urges secure and protected platform who use internet. Cyber security gives the facility to internet users access/use the secure and protected source and way. Intranet has a private network used in government organizations and especially in military. It is more secure as compared to local internet but some drawbacks are occurred in this network. Then onion routing and intelligent agents control/protect the all over system by any threats and attacks. The security is the fundamental issue in the versatile specially appointed system [18]. In MANNET hub looks like self-centeredness. A hub can utilize the assets of other hub and safeguard the assets of possess. This sort of hub makes the issue in MANET there is various ways, which ensure for the wellbeing and security of your system [19]. Play out the accompanying to keep away from security provisos must have a refreshed antivirus program; try not to give progressively or undesirable access to any system client. Working framework ought to be consistently refreshed.

## References

[1] Newman, S. (2017). Service providers: the gatekeepers of Internet security. Network Security, 2017, 5-7.

[2] Boshoff, W. H., & von Solms, S. H. (1989). A path context model for addressing security in potentially non-secure environments. Computers \& Security, 8, 417-425.

[3] Deibert, R. (2012). Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Journal of military and strategic studies, 14.

[4] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law \& Security Review, 32, 715-728.

[5] de Argaez, E. (2011). Internet world stats: Usage and population statistics. Internet world stats.

[6] Suhariyanto, B. (2012). Information and Technology Crime (Cybercrime). Jakarta, PT. RajaGrafindo Persada.

[7] Tawar, M., & Keshari, V. (2013). The Impact of Information Technology on Work and Society. Pioneer Journal, 12, 00.

[8] Goldschlag, D. M., Reed, M. G., & Syverson, P. F. (1996). Hiding routing information. International Workshop on Information Hiding, (pp. 137-150).

[9] Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.

[10] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53, 23-40.

[11] Ghaffari, A. (2006). Vulnerability and security of mobile ad hoc networks. Proceedings of the 6th WSEAS international conference on simulation, modelling and optimization, (pp. 124-129).

[12] Zhu, N., & Zhao, H. (2017). IoT applications in the ecological industry chain from information security and smart city perspectives. Computers \& Electrical Engineering.

[13] Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1996). Proxies for anonymous routing. Computer Security Applications Conference, 1996., 12th Annual, (pp. 95-104).

[14] Kompara, M., & Hölbl, M. (2018). Survey on security in intra-body area network communication. Ad Hoc Networks, 70, 23-43.

[15] Boshoff, W. H., & Von Solms, S. H. (1990). Application of a path context approach to computer security fundamentals. Information Age, 12, 83-90.

[16] Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.

[17] Chaudhry, P. E. (2017). The looming shadow of illicit trade on the internet. Business Horizons, 60, 77-89.

[18] Li, W., & Joshi, A. (2008). Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.

[19] Sharma, K., Khandelwal, N., & Prabhakar, M. (2010). An overview of security problems in manet. Proceedings of the International Conference on Network Protocols (ICNP).