International Journal of Civil Engineering and Technology (IJCIET)
Volume 9, Issue 6, June 2018, pp. 1583–1592, Article ID: IJCIET_09_06_178
Available online at http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=6
ISSN Print: 0976-6308 and ISSN Online: 0976-6316

THE PHENOMENON OF CYBER-CRIME AND FRAUD VICTIMIZATION IN ONLINE SHOP

Muhammad Dharma Tuah Putra Nasution, Andysah Putera Utama Siahaan, Yossie Rossanty, Solly Aryza
Universitas Pembangunan Panca Budi, Indonesia

ABSTRACT

Simple negligence can be a fatal impact. The threat of cyber in 2017 is feeble, and it starts from "wanna cry" until "nopetya" that the impact is relatively weak. The public also feels the threat of cybercrime even in many countries who have become the target of cyber-war, the society became the most disadvantaged. Cybercrimes have an impact on the National Security, financial loss and consumer confidence. Therefore, in the middle of the more high dependency, man will use information technology, cybersecurity must be the primary priority for a state. The Indonesian people still believe that only the information is available on the internet. Even though the information may unnecessarily is accurate. The results of a survey conducted by the CIGI Ipsos in 2016 released in 2017 shows that 65 percent of Indonesia receives the information is available on the internet without filtering the first.

Key words: Cybercrimes, Fraud Victimization, National Security, Financial Loss, Consumer Confidence.

Cite this Article: Muhammad Dharma Tuah Putra Nasution, Andysah Putera Utama Siahaan, Yossie Rossanty, Solly Aryza, The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop, International Journal of Civil Engineering and Technology, 9(6), 2018, pp. 1583–1592.
http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=9&IType=6

1. INTRODUCTION

Penetrate the borders now feels closer, so that the time to explore specific destinations is the faster. It may be called with the era where everyone can penetrate the space and time more quickly and easily [1], [2]. the Internet is a leading cause of this. The term Internet define as the collection of millions of computers that provide a network of electronic connections between the computers [3]–[6]. The Internet has developed into an essential channel for product purchase and orientation [7]–[11]. It is not surprising if the development of the internet in countries such as the United States, the United Kingdom, Germany, and the Netherlands have made the internet as media or the favorite marketing channels [12]–[14].

In addition to the sales of the product will be more easily and consumers can access more affordable to consumer goods, there is also the negative side from e-shopping that cause potential "fraud victimization." Each internet users have the risk of facing the dark side of the internet called cybercrime. The term cybercrime defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction [3]. Other words represent the cybercrime as the Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or online data, or sabotage of equipment and data [15]–[17]. During the year 2016, costly cybercrime grade globally reach USD 450 billion. That figure could continue to rise when the netizen, especially in a large city that many related to the business world and the government still has a low cyber awareness. Simple negligence can be fatal. The threat of cyber along 2017 is feeble, and it starts from wanna cry until nopetya that the impact is relatively weak. The public also began to feel the threat of cybercrime grade even in many countries who have become the target of war cyber; the society became the most disadvantaged.

In the middle of the more high dependency man will use information technology, security cyber of course must be the primary priority countries, before the more significant loss befell Indonesia. Based on a survey conducted by security institutions cyber CISSReC 2017, the level of consciousness cyber internet users in Indonesia is still considered low [18]. In the case of wanna cry, for example, societies tend to be ignorant of merely a proposal for the government to set up on a personal computer or laptop powered Windows. The case of hacker website Telkomsel and tiket.com is a small part of the example of the low-security level cyber in Indonesia. Should be from both the case can be made the lessons as well as a warning that the threat of cybercrime grade at in Indonesia is in front of the eye. The invaluable loss can occur when hacker successfully targets and paralyze critical object a country, including government service system, emergency service, the oil and gas reserves, finance and banking, transportation, telecommunications electrical energy, and irrigation system.

2. LITERATURE REVIEW

2.1. Cyber-Criminals

The Internet space or cyberspace is growing very fast and as the cyber crimes. Some of the kinds of Cyber-criminals are mentioned as;

- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters: These individuals perpetrate tricks on others. They do not intend any particular or long-lasting harm.
- Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases, they conspire with others or work within organized gangs such as the Mafia.
- Cyber terrorists: There are many forms of cyber terrorism. Sometimes it is a rather smart hacker breaking into a government website, other times it is just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others to the criminally negligent.

- Cyber bulls: Cyberbullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on websites, and mean or cruel email messages are all ways of cyberbullying.
- Salami attackers: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed, e.g., a bank employee inserts a program into bank‘s servers, which deducts a small amount from the account of every customer.

Meanwhile, cyber attacks the giant scale using the device hacker has attacked some institutions and organizations in the world. Related authorities in various countries have been trying to keep the network secure their computers by renewing the system from possible attacks hacker [19]–[21] Hacker groups are known as "The Shadow Brokers" claim to have stolen the appliance hacker and release of online. Some experts say the attacks likely have done to exploit the weakness of the Microsoft system that has been identifying and given the name EternalBlue NSA [22]–[24] The appliance hacker belongs to NSA then stolen a group of hackers who call themselves as The Shadow Brokers, who then try to sell it in an online auction. However, they then make the tools that are available freely. The hacker said they publish the password as "protest" against US President Donald Trump policy. During the number of cybersecurity experts has said that the attacking hacker is real, but it is unconsidered too frightening. Microsoft has released a system to cover the weakness of hacker attacks, but it could not be applied because it is not all system to perform an update [25]–[27].

Many organizations realize the needs of cyber security strategy will be capable of dealing with the risks that threaten their business. According to research from the System Engineer Web Fraud Protection (2016) stated that there is five cyber threat which is the most common for online business [28], [29].

2.2. Malware

Malware is the most frequently used criminals around the world to get access to the system and confidential data. In business online, operating mode is often were introduced into the regulatory e-commerce site to steal the data customers [30]–[32].

2.3. Application Attacks

Using the credentials and stolen information attacks are capable of targeting the vulnerabilities in a web application, especially on the site e-commerce and banking. Usually, the customer will be directed to a false web site that can suck up the personal information. This is the data that is often used by cybercriminals [33]–[35].

2.4. Botnet Attacks

This is a quite sophisticated scheme. To take advantage of the brute force attacks and algorithm and sophisticated botnet cybercriminals attempting to steal various data transaction belongs to the sacrifice, and selleth online [36]–[38].

2.5. Threat from the Company

The threat to the company itself also many happened. Access to the site of the company that is not so safe makes it easier for criminals to access a variety of data the secret of the company through the account of the employees [39]–[42].

2.6. Invasion of Traffic

Type of attack through high traffic is often used cyber-criminals to make a web network system overwhelmed. This type of attack is the most common done cybercriminals [43]–[45].

3. DISCUSSION

3.1. Impact of Cybercrimes

As reported the BBC Indonesia, Microsoft has released a special tool to prevent hacker attack, but haven t been because many systems that may not be updated. The report appears to mention hacker attack was hit 99 countries including the UK, USA, China, Russia, Spain, and Italy. The security company virtual world, Avast, said that he had seen the attack cyber as many as 75,000 cases in the whole world. They mention the attack named WCry or WannaCry.

Many researchers say that the incident this cyber attacks seems to be related to each other, but this possibility is not coordinated attacks against a specific target. Who is affected by the attack? The Ministry of Health in the UK and Scotland seems including institutions are reported to be affected by the most severe cyber attacks. Hacker attack appears in the computer through email and network, if opened will lock all files in the computer network. As a result of this attack, some activities in the hospital in England and Scotland should be suspended or canceled. Some reports say Russia is one of the most epic from this cyber attacks compared to other countries. The ministry in the land of Russia said it had localized the virus following the attacks on a personal computer using the Windows operating system.

Many community members have been uploading photos of the screen their computers that the epic hacker attack, including local train ticket machine in Germany and the computer laboratory at a university in Italy. Some of the companies in Spain, including telecommunication company Telefonica themes and power company Iberdrola, feel the impact of cyber attacks. There is a report which stated that the staff in some companies are told to turn off their computer. The company telecom Portugal, shipping company FedEx, as well as the second largest mobile phone network in Russia also claim that they had been impacted.

3.2. Impact of the Financial Loss

Nowadays Indonesia increased financial cybercrime and troubling, based on data from the Norton by Symantec in Indonesia in January 2015 until February 2016, recorded financial losses due to crime cyber reached Rp 7.6 million people per sacrifice and by the total loss in Indonesia reached Rp 194,6 billion. While based on data Central Bank, in 2007 the number of complaints customers who are victims of fraud by bank transfer as much as 2.558 cases with the value of fraud worth Rp3.4 billion. While in 2008, the number of complaints reached 6.347 cases with the value of fraud Rp19,4 billion, and 2009 as much as 6498 cases with the value of Rp62,9 billion. While 2010 until the first semester reached 694 cases with the value of Rp954 million, even the funds can be more substantial because usually the bank less transparent (closed) to communicate to the public and regulators because it is associated with the effect of the image of the banks. Besides, PwC survey titled Global Economic Crime Survey (2014), with involving as many 5.128 respondents from 95 countries interviewed between August and October 2013, found as much as 37 percent of respondents said they never become victims of economic crimes, three percent increases this figure from data 2011 and 56 percent of financial crimes involving the internal company.

3.3. Impact on Consumer Confidence

Cyber Crime create each of the average compensation USD 358 or total approximately USD 150 billion. So the findings of the Norton Cybersecurity Insights Report (2015), which highlighted the bitter reality of crime online and personal effects on consumers in 17 countries [11]. This report found that globally, 62 percent of consumers believe that the credit card information they will be stolen online, and 38 percent of respondents think that they will lose the credit card information from their wallets. Also, 47 percent reported they never affected by the impact of cybercrime. Shaken consumer confidence in the year 2014, when there is a huge transgression which has never happened before that expose the identity of the millions of people who only make routine purchases from retailers that already known, according to Lowth, joined destabilized the trust of the community in online activities [46]. However, the threat of cybercrime has not been encouraging the adoption of simple protection that must be done to protect their information online

[8]. Most do not perform necessary actions online security: use passwords. When these people too confident with the knowledge of security which they have to fear is the usual. As many as eighty percents felt that the opportunity to become the victim of a crime online quite significant for worried. According to a survey by Norton, victims of crime online the average lost time 21 hours due to deal with the impact of cybercrime. More than half of the consumers (60%), sure using WiFi more at risk than using the public toilet (40%).

3.4. Change the Habit of Internet Users

Excessive dependence on digital devices and the attitude of indifferent to the digital device security to the attention of the main areas of cybersecurity is affected in Kaspersky Cybersecurity Index. The latest survey Kaspersky Lab where is a number of the indicators designed to reflect changes in the behavior of internet users and the risk that they face.

In the first half of 2017 (H1 2017), the Index shows that the user increasingly mobile user even elderly also faced increasing danger online, and decrease the number of users who are protected by a security solution. Based on the results of the survey online internet users throughout the world, which is done twice a year by Kaspersky Lab. On H1 2017, a survey conducted among 21.081 users from 32 countries, aged 16 or more. The research found that the more modern users rarely use the computer for their online activities, but prefer to use mobile devices.

As an example of an e-mail, where 78% users access account e-mail them from their computer, the number is reduced from six months earlier that still reached 87%. 67% do so from mobile devices they have increased 59 percent in the second half of the year 2016. The number of users who use their mobile devices for shopping online has increased to 50% from 41 percent compared to the previous six months, while users were shopping online from the computer experiencing a decline from 80% to 75%. This trend is observed in most types of online activity is monitored in the index. In the last few years, the average number of devices per household shows declined slightly-mainly due to the reduction in the number of computers per household.

3.5. Impact of Changes in Habits

This can be associated with the fact that the user is increasingly using their mobile devices, which often does not have the protection when compared to their computers. This is a dangerous trend: users face risk when using mobile devices, and the more often they use it for online activity, the higher the risks.

This time Android users face ransomware program that can encrypt the user data on their telephone in return for a ransom; malware that aims to steal money from mobile banking application; and phishing web page that is designed to get the forbidden access to user accounts, for example in social networking. Based on the report Kaspersky Lab shows that every four (27%) respondents reported they had become victims of cybercriminals, in some types of digital devices.

Elderly users (aged 55 or more) find themselves at risk of higher on H1 2017. While in H2 2016 only 12% users in the age that reported that they face the threat of online, on H1 has no 19% users who reported that they are dealing with some types of malware. Regardless of the age and the work of a user, focus their digital life more switches to mobile devices - The user trusts the secret files, confidential information, money and many other things into the mobile devices belonging to them. However, the criminal's virtual world is not silent and alter their tactics to more often offensive to the mobile platform.

3.6. The Merit of Digital Literacy

Indonesian people still believe that only the information that is available on the internet, even though the information may be not necessarily valid. Quoting the results of a survey conducted by the CIGI Ipsos in 2016 released on 2017. Contents, 65% of Indonesia swallowed up the crude prices information is available on the internet. As information, internet users in Indonesia based on the results of the study of the Association of Indonesian Internet Service Provider in 2016 in numbers 132,7 million. While, CIGI-Ipsos derived Canada cooperate with some institutions that take samples in 24 countries, including Indonesia. From the results of the survey, 15 percent of society directly believe, 50 percent believed, so there was a total of 65 percent who believe the information on the internet. This is put Indonesia in a position to seven. 65 percent of the total internet users that 132 million, believed that the information on the internet. This condition is hazardous if the digital literacy does not follow it. See the condition of the government, in this case, the Ministry of communication and information literacy increased in the digital community. The purpose can overcome the harmful content such as hoax, radicalism, pornography and so on. The impact of technology on literacy rate can cause delirium in the community where the content can be in manufacturing, and it is dangerous. The form of digital literacy by the Government is done with the collaboration and involvement of the Related Party, make the curriculum about digital, community empowerment of the community that serves as a 'lanterns' in the community until the cyber governance. At this time the high control but low literacy. Later, when the high literacy low control, therefore control the most effective. At the time of the exposed with negative content, they have been able to control themselves.

4. CONCLUSIONS

This manuscript is merely not only on the understanding of cybercrime but also explains the impact of various levels of society [13]. It will help people to secure all information online critical organization is not secure because of the cybercrime like that. The understanding of the behavior of cybercrime and the impact of cybercrime on the community will help to know how to resolve the adequate situation. The way to overcome this crime can be classified into three categories: Cyber Law, education and policy-making. All of the above ways to handle this cybercrime has very little important work or have nothing in many countries. The lack of work is needed to improve the work that already exists or to set up a new paradigm for control of cyber attacks.

Cybercrime is the attack against the content, computer system and communication system owned by other people or general in cyberspace. The phenomenon of cybercrime is quite different from other crimes in general. Cybercrime can be done without know the territorial boundaries and does not require direct interaction between the perpetrators with victims of crime. Therefore, the integrated security system is needed to close the existence of these gaps in illegal actions that harm. Personally, security can be done starting from the installation of the system until finally toward the stage of physical security and data security. The Organization for Economic Cooperation and Development (OECD) provides some essential steps that must be done in every country in combating cybercrime be :

- Do the modernization of national criminal law and the law of excellence.
- Improve national computer network security system according to the international standards.
- Improve the understanding and expertise of the legal enforcement apparatus about prevention efforts, investigations and prosecution of matters related to cybercrime.
- To increase the awareness of the citizens of the problem and the importance of preventing cybercrime occurred.
- Improve the intergovernmental cooperation, bilateral, regional and multilateral organizations in the efforts of cybercrime handling.

The need for the support particular Institutions owned by the government and NGO (Non-Government Organization), as an effort to tackle the crime on the internet. The United States has the Computer Crime and Intellectual Property Section (CCIPS) as a specific division of the U.S. The Ministry of Justice. This institution provides information about cybercrime, making socialization intensively to the community as well as doing research on special research in combating cybercrime.

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support from Universitas Pembangunan Panca Budi, and we would like to thank the anonymous reviewers for their comment on this article.

REFERENCES

[1] S. Aryza, A. N. Abdalla, Z. Khalidin, and Z. Lubis, “Adaptive Speed Estimation of induction motor Based on Neural network Inverse Control,” Procedia Eng., vol. 15, pp. 4188–4193, 2011.

[2] R. Rahim, T. Afriliansyah, H. Winata, D. Nofriansyah, Ratnadewi, and S. Aryza, “Research of Face Recognition with Fisher Linear Discriminant,” IOP Conf. Ser. Mater. Sci. Eng., vol. 300, p. 012037, Jan. 2018.

[3] H. Saini, Y. S. Rao, and T. C. Panda, “Cyber-Crimes and their Impacts: A Review,” Int. J. Eng. Res., vol. 2, no. 2, pp. 202–209, 2012.

[4] A. P. U. Siahaan and R. Rahim, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” Int. J. Secur. Its Appl., vol. 10, no. 8, pp. 173–180, Aug. 2016.

[5] S. Aryza, M. Irwanto, Z. Lubis, A. P. U. Siahaan, R. Rahim, and M. Furqan, “A Novelty Design of Minimization of Electrical Losses in A Vector Controlled Induction Machine Drive,” in IOP Conference Series: Materials Science and Engineering, 2018, vol. 300, no. 1.

[6] Y. Rossanty, D. Hasibuan, J. Napitupulu, M. D. T. P. Nasution, and R. Rahim, “Composite performance index as decision support method for multi case problem,” Int. J. Eng. Technol., vol. 7, no. 2.29, pp. 33–36, 2018.

[7] K. A. Saban, E. McGivern, and J. N. Saykiewicz, “A Critical Look at the Impact of Cybercrime on Consumer Internet Behavior,” J. Mark. Theory Pract., vol. 10, no. 2, pp. 29–37, Apr. 2002.

[8] A. D. Smith, “Cybercriminal impacts on online business and consumer confidence,” Online Inf. Rev., vol. 28, no. 3, pp. 224–234, Jun. 2004.

[9] Y. M. Saragih and A. P. U. Siahaan, “Cyber Crime Prevention Strategy in Indonesia,” SSRG Int. J. Humanit. Soc. Sci., vol. 3, no. 6, pp. 22–26, 2016.

[10] R. Rahim et al., “Searching Process with Raita Algorithm and its Application,” J. Phys. Conf. Ser., vol. 1007, no. 1, pp. 1–7, 2018.

[11] M. Dharma Tuah Putra Nasution et al., “Decision Support Rating System with Analytical Hierarchy Process Method,” Int. J. Eng. Technol., vol. 7, no. 2.3, pp. 105–108, Mar. 2018.

[12] J. van Wilsem, “‘Bought it, but Never Got it’ Assessing Risk Factors for Online Consumer Fraud Victimization,” Eur. Sociol. Rev., vol. 29, no. 2, pp. 168–178, Apr. 2013.

[13] M. D. T. P. Nasution and Y. Rossanty, “Country of Origin as a Moderator of Halal Label and Purchase Behavior,” J. Bus. Retail Manag. Res., vol. 12, no. 2, pp. 194–201, 2018.

[14] R. Rahim et al., “Combination Base64 Algorithm and EOF Technique for Steganography,” J. Phys. Conf. Ser., vol. 1007, no. 1, pp. 1–5, 2018.

[15] A. P. U. Siahaan, “Pelanggaran Cybercrime dan Kekuatan Yuridiksi di Indonesia,” J. Tek. dan Inform., vol. 5, no. 1, pp. 6–9, 2018.

[16] S. Ramadhani, Y. M. Saragih, R. Rahim, and A. P. U. Siahaan, “Post-Genesis Digital Forensics Investigation,” Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 164–166, 2017.

[17] A. Lubis and A. P. U. Siahaan, “Network Forensic Application in General Cases,” IOSR J. Comput. Eng., vol. 18, no. 6, pp. 41–44, 2016.

[18] A. P. U. Siahaan et al., “Combination of Levenshtein Distance and Rabin-Karp to Improve the Accuracy of Document Equivalence Level,” Int. J. Eng. Technol., vol. 7, no. 2.27, pp. 17–21, 2018.

[19] M. Saragih, H. Aspan, and A. P. U. Siahaan, “Violations of Cybercrime and the Strength of Jurisdiction in Indonesia,” Int. J. Humanit. Soc. Stud., vol. 5, no. 12, pp. 209–214, 2017.

[20] H. A. Dawood, “Graph Theory and Cyber Security,” in 2014 3rd International Conference on Advanced Computer Science Applications and Technologies, 2014, pp. 90–96.

[21] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, “Cybercriminals, cyberattacks and cybercrime,” in 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, pp. 1–9.

[22] K. Veena and P. Visu, “Detection of cyber crime: An approach using the lie detection technique and methods to solve it,” in 2016 International Conference on Information Communication and Embedded Systems (ICICES), 2016, pp. 1–6.

[23] D. J. Neufeld, “Understanding Cybercrime,” in 2010 43rd Hawaii International Conference on System Sciences, 2010, pp. 1–10.

[24] N. Kshetri, “The simple economics of cybercrimes,” IEEE Secur. Priv. Mag., vol. 4, no. 1, pp. 33–39, Jan. 2006.

[25] M. den Hengst and M. Warnier, “Cyber Crime in Privately Held Information Systems: Personal Data at Stake,” in 2013 European Intelligence and Security Informatics Conference, 2013, pp. 117–120.

[26] S. Ullah, M. Amir, M. Khan, H. Asmat, and K. Habib, “Pakistan and cyber crimes: Problems and preventions,” in 2015 First International Conference on Anti-Cybercrime (ICACC), 2015, pp. 1–6.

[27] H. M. Ritonga, H. A. Hasibuan, and A. P. U. Siahaan, “Credit Assessment in Determining The Feasibility of Debtors Using Profile Matching,” Int. J. Bus. Manag. Invent., vol. 6, no. 1, pp. 73–79, 2017.

[28] X. Fu, Z. Ling, W. Yu, and J. Luo, “Cyber Crime Scene Investigations (C^2SI) through Cloud Computing,” in 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, 2010, pp. 26–31.

[29] Y. Rossanty and M. D. T. P. Nasution, “Information Search and Intentions to Purchase: The Role of Country of Origin Image, Product Knowledge, and Product Involvement,” J. Theor. Appl. Inf. Technol., vol. 96, no. 10, pp. 3075–3085, 2018.

[30] D. Gavrilut, M. Cimpoesu, D. Anton, and L. Ciortuz, “Malware detection using machine learning,” in 2009 International Multiconference on Computer Science and Information Technology, 2009, pp. 735–741.

[31] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, “Malware classification with recurrent networks,” in 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2015, pp. 1916–1920.

[32] V. Tasril, M. B. Ginting, Mardiana, and A. P. U. Siahaan, “Threats of Computer System and its Prevention,” Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 448–451, 2017.

[33] O. B. Al-Khurafi and M. A. Al-Ahmad, “Survey of Web Application Vulnerability Attacks,” in 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2015, pp. 154–158.

[34] S. Nanda, L.-C. Lam, and T.-C. Chiueh, “Web Application Attack Prevention for Tiered Internet Services,” in 2008 The Fourth International Conference on Information Assurance and Security, 2008, pp. 186–191.

[35] Hariyanto and A. P. U. Siahaan, “Intrusion Detection System in Network Forensic Analysis and,” IOSR J. Comput. Eng., vol. 18, no. 6, pp. 115–121, 2016.

[36] L. Zhang, S. Yu, D. Wu, and P. Watters, “A Survey on Latest Botnet Attack and Defense,” in 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp. 53–60.

[37] Ying Wang, Zhigang Jin, and Wei Zhang, “Analysis of Botnet attack and defense technology,” in 2011 International Conference on Computer Science and Service System (CSSS), 2011, pp. 3021–3023.

[38] Haryanto, A. P. U. Siahaan, R. Rahim, and Mesran, “Internet Protocol Security as the Network Cryptography System,” Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 223–226, 2017.

[39] J. R. C. Nurse et al., “Understanding Insider Threat: A Framework for Characterising Attacks,” in 2014 IEEE Security and Privacy Workshops, 2014, pp. 214–228.

[40] H. Chi, C. Scarllet, Z. G. Prodanoff, and D. Hubbard, “Determining predisposition to insider threat activities by using text analysis,” in 2016 Future Technologies Conference (FTC), 2016, pp. 985–990.

[41] S. Shamov, A. Sarbash, and S. Florov, “Means of countering threats in communication systems of broker companies,” in 2017 4th International Scientific-Practical Conference

Problems of Infocommunications. Science and Technology (PIC S&T), 2017, pp. 187–192.

[42] R. D. Sari, Supiyandi, A. P. U. Siahaan, M. Muttaqin, and R. B. Ginting, “A Review of IP and MAC Address Filtering in Wireless Network Security,” Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 470–473, 2017.

[43] S. W. Lodin and C. L. Schuba, “Firewalls fend off invasions from the Net,” IEEE Spectr., vol. 35, no. 2, pp. 26–34, Feb. 1998.

[44] H. Ming and S. LiZhong, “A New System Design of Network Invasion Forensics,” in 2009 Second International Conference on Computer and Electrical Engineering, 2009, pp. 596–599.

[45] M. D. L. Siahaan, M. S. Panjaitan, and A. P. U. Siahaan, “MikroTik Bandwidth Management to Gain the Users Prosperity Prevalent,” Int. J. Eng. Trends Technol., vol. 42, no. 5, pp. 218–222, 2016.

[46] I. B. Hong and H. Cho, “The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust,” Int. J. Inf. Manage., vol. 31, no. 5, pp. 469–479, Oct. 2011.

[47] N. Srihari Rao, Prof. K. Chandra Sekharaiah and Prof. A. Ananda Rao , An Approach to Dis tinguish the Conditions of Flash Crowd Versus Ddos Attacks and to Remedy a Cyber Crime . International Journal of Computer Engineering and Technology, 9(2), 2018, pp. 1 1 0 - 123

[48] Prashant Mali, J.S. Sodhi, Triveni Singh, Sanjeev Bansal , Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study , International Journal of Mechanical Engineering and Technology 9(2), 2018, pp. 110 – 124