International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 12, Issue 4 (Jul.-Aug. 2023), PP. 71-77

Review on Cyber-security

Subhadra Biswal[1] Jharana Paikaray[2] Biswajit Tripathy[3] Sujata Behera[4]
[1,2,3,4] *Department of Computer Science and Engineering, Einstein Academy of Technology & Management, Bhubaneswar*

Abstract
A qualitative study conducted in Korea reveals that businesses use security techniques to protect their information systems, with a focus on preventing security threats using technological countermeasures. The study found a deep-rooted preventative mindset driven by the desire to ensure technology availability and a lack of awareness of enterprise security concerns. The research agenda for deploying multiple strategies across an enterprise includes combining, balancing, and optimizing systems. Nine security strategies were identified, and a qualitative focus group approach was used to determine their use in organizations. Many organizations use a preventive approach to keep technology services available, while some other methods support the prevention strategy on an operational level.

Keywords: Cybersecurity; Cyberspace; Cyber terrorism

I. Introduction

Today an individual can receive and send any information may be video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue (Dervojeda, et. all., 2014). The extent of cybersecurity does not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. Improving cybersecurity and ensuring that necessary data systems are vital to each country's security and financial prosperity. Creating the Internet safer (and safeguarding Internet clients) has become to be essential to the improvement of new management just as a legislative strategy. The encounter against cybercrime needs an extensive and more secure practice (Gross, Canetti &Vashdi, 2017). The particular estimates alone cannot keep any crime; it is essential that law authorization offices are allowable to investigation and indict cybercrime efficiently. Nowadays numerous countries and administrations are compelling strict rules on cyber safeties to keep the loss of some vital data. Each should be equipped onthiscybersecurity and save themselves from these increasing cybercrimes.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure (Kumar, & Somani, 2018). It alludes to a lot of exercises and measures, both specialized and non-specialized, expected to ensure the bioelectrical condition and the information it contains and transports from all possible threats. This research aims to gather all the information and overview related to cyber-crime and provide the historical facts and perform reports on the analyzed data of different attacks reported everywhere in the last five years. Based on the analyzed information, we would like to provide all the countermeasures that organizations may undertake in order to ensure improved security that would , we would like to provide all the countermeasures that organizations may undertake in order to ensure improved security that would support in defending the organizations from being attacked by the hackers and provide a cyber-security to avoid all risks.support in defending the organizations from being attacked by the hackers and provide a cyber-security to avoid all risks.

II. Purpose

The paper provides information about cyber security and cyber terrorism. It covers various information about these topics in its subsections. Trends of cybersecurity and the role of social media in cybersecurity define in this paper. The paper provides some necessary information about cyber terrorism. The components of "cyber terrorism" and the consequences of this terrorism also explain in this paper. There are some examples of case studies those related to cybersecurity. The paper also provides some solutions regarding cyber security and cyber terrorism. It provides some techniques for preventing cyber terrorism. The future study and scope of cybersecurity define in it. Cybersecurity has become a major concern over the last 10 year in the IT world. In the present world, everybody is facing a lot of problems with cybercrime. As hackers are hacking major sensitive information from government and some enterprise organizations the individuals are very much worried

as cybersecurity assault can bring about everything from wholesale fraud, to blackmail big companies. They are many varieties of cyber-crimes emerging where everyone needs to be aware of the scams and they are different measures and tools which can be used for avoiding the cyber-crimes. Every organization wants to secure their confidential data from getting hacked. Getting hacked is not just about losing the confidential data but losing the relationship with customers in the market (Bendovschi, 2015). The Internet is today's fastest growing infrastructure. In today's technical environment many new technologies are changing mankind. But due to these emerging technologies, we are unable to protect our private information in an efficient way, so the cyber-crimes are drastically increasing on daily basis.

Majority of the transactions both commercial and personal are done using the means online transaction, so it is important to have an expertise who require a high quality of security maintaining a better transparency to everyone and having safer transactions. So cybersecurity is the latest issue. Advanced technologies like cloud services, mobiles, E-commerce, internet banking and many more they require a high standards and safer process of security. All the tools and technologies involved for these transactions hold the most sensitive and crucial user information. So providing the necessary security to them is very important. Improving the cybersecurity and safeguarding the sensitive data and infrastructures are important to every countries top priority security (Panchanatham, 2015)

III. Trends of Cyber Security

Cyber Security assumes a critical role in the area of data technology. Safeguarding the data have become the greatest difficulty in the current day. The cybersecurity the main thing that raids a chord is cybercrimes which are increasing tremendously step by step (Samuel, & Osman, 2014). Different administrations and organizations are taking many measures to keep these cybercrimes. Additional the different measures cybersecurity is as yet an enormous worry to numerous. Some main trends that are changing cybersecurity give as follows:

3.1. Web servers

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web serversas well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

3.2. Mobile Networks

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

3.3. Encryption

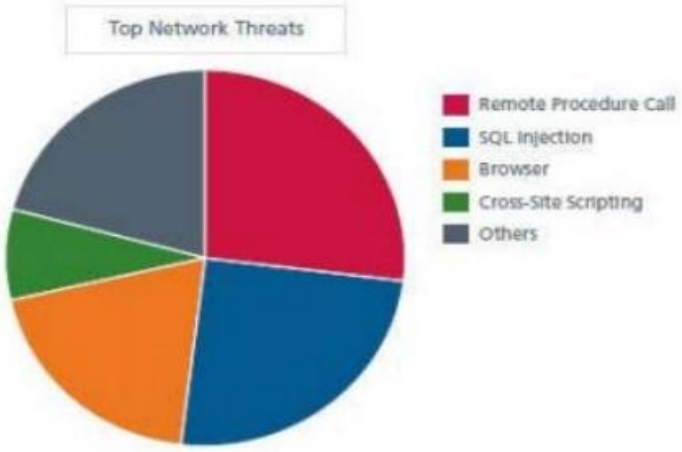
It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into a stirred-up figure content. It commonly completes with the use of an "encryption key," that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability (Sharma, 2012). Additional use of encryption obtains more problems in cybersecurity. Encryption is used to ensure the information in travel, for instance, the information being exchanged using systems (for example the Internet, online business), mobile phones, wireless radios and so on.

3.4. ADP's and targeted attacks

Advanced PersistentThreat (APT) is a whole of the dimension of cybercrime ware. For quite a long time network security capacities. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults (Bendovschi, 2015). As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion

of the patterns.changing the essence of cybersecurity on the planet. The top network threats are showing in figure 1.

Figure 1. Threats for Cyber Security



IV. Role of Social Media

in Cyber Security social media has turned into a lifestyle for some individuals. We use it to stay in contact, plan occasions, share our photographs and comment on recent developments. It has replaced email and telephone requires a ton of us. However, similarly as with whatever else on the web, it is imperative to know about the dangers. PCs, cell phones, and different gadgets are priceless assets that furnish people of any age with the extraordinary capacity to connect and collaborate with whatever remains of the world. Individuals can do this in various ways, including the utilization of social media or networking sites. Courtesy of social media, people can share musings, pictures, exercises, or any part of their lives (Gross, Canetti &Vashdi, 2017). They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. Unfortunately, these networks additionally represent security toward one's PC, protection, and even their security. Social media collection among faculty is soaring as is the risk of assault (Sharma, 2012). Since social media sites are nearly utilized by the majority of them reliably, it has become an excellent stage for cybercriminals for hacking private data and taking significant data.

The organizations need to assure they are likewise as fast in recognizing dangers, reacting increasingly, and keeping away from a rupture of any sort. Subsequently, individuals must take suitable measures particularly in managing social media to keep the loss of their data. The capacity of persons to impart data to a group of persons of millions is at the core of the exact test that social media offerings to organizations (Cabaj, Kotulski, Księżopolski, &Mazurczyk, 2018). Nevertheless, enabling anyone to disperse financially delicate data, social media additionally gives a comparable ability to range false data. It can be merely being as harming. The rapid spread of incorrect information by social media is among the growing dangers. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. In its place, they should have arrangements that will inform them of the risk to fix it before any actual harm is done Dervojeda, Verzijl, Nagtegaal, Lengton, &Rouwmaat, 2014). Anyway, organizations should understand this and observe the meaning of breaking down the data chiefly in social deliberations and give good security plans to avoid dangers. One must contract with social media by using specific plans and the right technologies.

V. Cyber Terrorism

The term “terrorism” can allude to the illegal utilization of power or viciousness against people in order to threaten an administration or its residents and associations which might be to accomplish a political or a malicious site [10]. Terrorism has transformed from the conventional structure to the cyber type of innovation supported terrorism recognized as cyber terrorism. It stays vital issues of the present society. Not just that the battle against terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational (Sharma, 2012). This terrorism is the utilization of cyber word to dispatch an assault to the essential foundations that the presence of associations and countries entirely depended after that can prompt its shut down

5.1. Components of Cyber Terrorism

A few attacks as cyber terrorism have a few parts which have been distinguished by numerous observational researchers in the exploration network. As indicated by Samuel and Osman (2014) in their hypothetical model recognize the five sections that a "cyber-terrorism" classified they are; the objective of the violence, inspiration and dedication towards the mission to be accomplished when such incident takes place, impact, instruments are utilized to dispatch such assaultand attacking's, area which is nature just as the strategy for activity. It can confidently know by knowing the profile of activities that drive the actions of the culprits (Kumar, & Somani, 2018). The critical issue in "cyber terrorism" is the motivation to complete such an action on the Internet, that outcomes in savagery/damage to people and their property Dervojeda, Verzijl, Nagtegaal, Lengton, &Rouwmaat, 2014). It is by a portion of the segments. The terrorists of the world proceed the upside of the cyber world with solid incentive as a stage with which they can use to dispatch more unusual outbreak. Yunos and Ahmad (2014) said that with the utilization of Information and correspondence innovation, a terrorist could present more noteworthy harms or exact the republic with troublesome conditions because of the interruption of necessary administrations that the "cyberspace terrorist" causes more damage and devastation by the cyberspace than done the conventional strategy for terrorism.

5.2. Motivating Factor of Cyber Terrorism

The motivating factors of cyber terrorism give as follows:

5.2.1. Websites' Supportive Nature:

The internet has viewed as a medium that is exceptionally tremendous, and that can in the meantime draw in light of a legitimate concern for some individuals to join some group of interest. The cyberterrorist prefers the utilization of the website as a result of its robust nature in that it can refer a message to a great many individuals inside a twinkle of an eye; they consider it to be a stage that is anything but difficult to select absorbed individuals.

5.2.2. Anonymity Nature of the internet:

Anonymity is the pivotal element that each evil culprit leans towards with the goal that their character could not be recognizable after playing out their devilish act. The Internet is a sheltered domain just as concealing stage for the terrorist as they can stay unknown so that their personality cannot be known.

5.2.3. Hacking:

The overall term of all kinds of unapproved access to any "computer system" network organize is hacking that can occur in any structure all things measured as "cyber murder." A large number of these hackers make use of a "brute force‟ which is the combinations of every single imaginable letter just as numbers and images till they get the password Sreenu, & Krishna, 2017

5.2.4. Computer Viruses:

These viruses are here and there scattered on a system to in other to do hurtful exercises. These may be to fill in as an administrative agent, create information or even split down the system.

5.2.5. Password Sniffing:

The "Cyber terrorist" may use one of the technique such as password sniff as procedures to complete their "cyber-attack" on different countries and many big organizations to see their downfall and have control over their systems. The password sniffer is programming which uses to screen organize and in the meantime catch all the password that passes the system connector

5.3. Consequences of "Cyber Terrorism"

Cyber terrorism is an original type of cyber danger and attack that has many outcomes connected to it when propelled against any countries and associations. Some consequences of cyber terrorism define as follows

5.3.1. Data Intrusion:

The cyber terrorism can annihilate information honesty with the goal that the information could never again be trusted, pulverizing its classification as intruding on its accessibility. The expanding rate of this cyber terrorism in encroaching associations and country's information has produced a ton of difficulties which has come about in loss of vitals and critical information that is typically difficult to recover (Sutton, 2017).

5.3.2. The attack on Businesses:

The cyber-terrorism could make associations lose billions of dollars in the region of organizations. The data arrangement of a bank can be attacked or hack through the terrorists who will prompt unapproved access to such financial balance and make them lose gigantic millions of dollars which can create such bank to keep running into bankruptcy (Gade, & Reddy, 2014).

5.3.3. Loss of Life:
Cyber terrorism has guaranteed many acquitted lives and in the meantime render numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. The "cyber-terrorism" can in one method or alternate prompts the death toll just as causing severe harms. It has shown in an attack on the PCs utilization, networks' as well as attacks that have 122 Unaut6. Case Study Examples

6.1. Cyber Security in E-Governance case study
E-Governance is the extension of the efforts completed through the governments to recover relations with their nationals. With its instilled straightforwardness and receptiveness, given the standards of the Internet, EGovernance conveys governments all the more near their residents. Existing and potential dangers in the circle of cybersecurity are among the most genuine difficulties of the 21st century. To ensure E-Governance extends there is a requirement for data security best practices (Hua, & Bapna, 2013). Security policies, practices, and techniques must be set up just as the use of security technology. It helps to ensure e-Government systems against attack, recognizes great exercises administrations and to have a demonstrated alternate course of action set up. An open private organization is a vital part of cybersecurity in EGovernance. These associations can conveniently go up against coordination issues. Powerful cyber-crime prevention and arraignment activities in all the ICT appropriate conditions.

6.2. Kaspersky Kidnapping Case
The "highest-profile" cyber surveillance, stalking, and kidnapping case included Ivan Kaspersky, child of the administrator and CEO of Russia-based Kaspersky Lab, a standout amongst the most unmistakable cybersecurity firms on the planet. Ivan Kaspersky was abducted for payoff in 2011 while strolling to work from his Moscow loft. As indicated by Russian media sources, beginners – a more seasoned obligated couple – organized the plot and enrolled their child and two of his companions as "muscle" for the plot (Cabaj, Kotulski, Księżopolski, &Mazurczyk, 2018). The abductors stalked Kaspersky and his sweetheart for a while preceding the seizing, deciding his conduct standards and finding that he did not 123 Unauthentifiziert | Heruntergeladen 01.09.19 21:18 UTC HOLISTICA Vol 10, Issue 2, 2019 have a protective security detail. The hijackers supposedly acquired all the required data from Kaspersky's client profile on Vkontakte, a famous Russian social systems administration site. Kaspersky was compelled to call his dad to transfer the payoff requests (Gade, & Reddy, 2014). The abductors may have utilized similar wireless to make food deliveries or had geolocation administrations empowered.

6.3. Uber Case study
Data breaches happen every day, in too many places, but the risk of data breach doesn't necessarily depend on the number, it may also depend on the risk and damage it causes the company's revenue and impact on the users or account holders, one of the biggest recent data breaches is Uber.

6.3.1. Impact:
One of the recent major cyber-attack is data breach of personal information of around 57million Uber users and 600,000 Uber drivers got revealed.

6.3.2. Details:
The worst part of this attack is how the Uber handled the issue, this is a lesson to most companies what not to do. In late 2016 just two hackers were able to steel the Users personal data with includes names, phone numbers and email addresses. They were able to steal the 600,000 driver's license information. Hackers got access to the Uber's GitHub account through a third-party cloudbased service. With the details found from the GitHub, Hackers found a way to access Uber user data in AWS. Ubers paid those two hackers $100, 000 to permanently destroy the whole data they obtained and not letting the users or the regulators about stolen information. But also, Uber confirmed that data was destroyed with the assurance they received from the hackers. According to US Law enforcement, any breach should be reported to the authorities and not pay hackers. And this kind of approach from Uber led other hackers to blackmail Netflix, where Hackers frightened to release TV shows unless the company paid the money hackers requested. Almost 49 states have this law enforcement where a security breach should be notified, after the court hearings Uber agreed to pay 20million to settle FTC charges. Not only the US but also other major countries like UK, Italy, and the Philippines reacted on this 124 Unauthentifiziert | Heruntergeladen 01.09.19 21:18 UTC HOLISTICA Vol 10, . Uber's breach is different from the regular breaches, the company tried to cover up the breach and not alert the authorities and the users.

6.3.3. Uber's plan after the breach:

Khrosrowshabi the new CEO of Uber received few disputed problems only with respect to its legal issue also criticism for sexual harassment, underpaying the drivers and few more.

6.3.4. Solutions Some solutions regarding cyber security and cyber terrorism describe here: • Cyber Security Techniques Some techniques can use to improve cybersecurity. • Access control and "password security": The idea of password and user name has a primary method for ensuring data. It may be the principal measures concerning cybersecurity. • Data's Authentication: The documents that we get should dependably be validated be before transferring. It should check if it has begun from a critical and dependable source and that they are not modified (Gade, & Reddy, 2014). Verifying of these records is typically done by the "antivirus" software present in the gadgets. Subsequently, a decent "antivirus" software is likewise necessary to shield the gadgets from viruses. • Anti-virus software: It is a PC program that classifies, avoids, and makes a move to harm or evacuate noxious software programs, for instance, viruses as well as worms. Most "antivirus programs" comprise an "autoupdate" feature that authorizes the program to download profiles of new viruses with the objective that it can chequer for the new viruses when they find.

• Malware scanners: This is software that typically filters each of the records and archives current in the framework for vindictive code or destructive viruses [10]. Viruses, worms, as well as Trojan horses, are instances of "malicious software" that regularly assemble and alluded to as malware.

• Firewall: A "software program" or an equipment that helps monitor hackers, infections, and all types of worms which endeavour to achieve PC over the Internet. All data which is transmitting to and fro over the web go through the firewall contemporary, which looks at every

6.4. Prevention of Cyber Terrorism The capacity to prevent cyber terrorism lies with the capacity to securely verify cyberspace. Cybersecurity has an intriguing parallel to terrorism. Both are lopsided. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a framework. The attacker has an inalienable preferred standpoint in both regular terrorism and cyber-attacks. On account of state-supported attacks, the difficulties are of a lot higher greatness (Cabaj, Kotulski, Księżopolski, &Mazurczyk, 2018). Governments should guarantee that their rules smear to cybercrimes and be wholly actualized and hold fast to; it is essential that the countries of the biosphere take measures to guarantee that its punitive and technical law is satisfactory to address the difficulties presented by cybercrimes (Kumar, &Somani, 2018). The availability, confidentiality and the integrity of information in any associations are essential which endeavors must be set up to guarantee that they are exceptionally secure because it is the significant cyber resource that makes each association stand and in the meantime depended upon. The information has entered by the "cyber-terrorist" is something beyond records which may incorporate messages, web applications, web pages, and just as some indispensable operating systems. (Kumar, & Somani, 2018) 7. Future Study and Scope This paper will help to advance the scientific interests in the exploration of cybersecurity, particularly to respond to the procedural questions of the prediction of future data and actions significant to security patterns. This study sets the background to begin executing rules for all intentions as indicated through the usual security issues and answers for data systems. This paper consolidates many procedures connected and may be improved to serve cybersecurity regarding anticipating the operational legitimacy of the methodologies of assessment benchmarks. Finally, the emphasis on limiting, recouping, and disposing of weakness is the primary, basic patterns, and reactions to the constant expanding progress (Panchanatham, 2015). 126 Unauthentifiziert | Heruntergeladen 01.09.19 21:18 UTC HOLISTICA Vol 10, Issue 2, 2019 Over the next five years, cyber-crime may create severe damage in information technology. According to the researchers they have estimated an approximate close to 6 trillion dollars loss. So, there would be a very bright scope for people who work and resolve the issues related to cyber-crime and provide all the necessary security measures. Big organizations like CISCO which is completely related to networking technology which is one of the top organization has approximately millions of openings related to cybersecurity because which is the future for the safety of Information technology. They are also wide opportunities in government-related fields and also defense field to save the countries secure data from cyber attackers. 8. Conclusion Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. The "cyber-terrorism" can in one method or alternate prompts the death toll just as causing severe harms. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. Cyber terrorism has guaranteed numerous innocent lives and in the meantime render numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. Cyber terrorism stays vital issues of the present society. Not just that the battle against Cyber terrorism is falling behind, current cybercrime assaults are ending up

progressively forceful and confrontational. Cybersecurity has an intriguing parallel to terrorism. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a system.

References

[1]. Bendovschi, A. (2015) Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077

[2]. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635- 018-0080-0 127 Unauthentifiziert | Heruntergeladen 01.09.19 21:18 UTC HOLISTICA Vol 10, Issue 2, 2019

[3]. Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., &Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.

[4]. Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[5]. Gross, M. L., Canetti, D., &Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

[6]. Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.

[7]. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.

[8]. Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

[9]. Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.

[10]. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).

[11]. Sreenu, M., & Krishna, D. V. (2017). A General Study on Cyber-Attacks on Social Networks. IOSR Journal of Computer Engineering (IOSR-JCE), 19(5), pp. 01-04. [12] Sutton, D. (2017).