Md Raju Biswas

by Iftekhar Efat

Submission date: 13-Mar-2022 12:41AM (UTC-0500)
Submission ID: 1782969730
File name: ASH1925001M.pdf (1.11M)
Word count: 4379
Character count: 24156

The most prominent pandemics of cyber viruses

Md Raju Biswas
ASH1925001M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

Technology is rapidly evolving in a world driven by social networks, online transactions, cloud computing, and automated processes. But with the technological evolution comes the progress of cybercrime, which continually develops new attack types, tools and techniques that allow attackers to penetrate more complex or well-controlled environments, and produce increased damage and even remain untraceable. The present article aims to get an overview of the cyber-crime as it is defined and revealed by specialized literature, international legislation and historical facts, and perform an analysis of attacks reported all around the world over the last three years in order to determine patterns and trends in cyber-crime. Based on the results of the analysis, the article presents the various virus of cyber attack on several option.Threats are generally much easier to list than to describe, and much easier to describe than to measure. As a result, many organizations list threats. Fewer describe them in useful terms, and still fewer measure them in meaningful ways. This is particularly true in the dynamic and nebulous domain of cyber threats—a domain that tends to resist easy measurement and, in some cases, appears to defy any measurement.

1 Introduction

1.1 Sub Intro

In a world driven more and more by big data, social networks, online transactions, information stored or managed via internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of number of attacks and level of damage caused to its victims.

There are many tools and way to hack and attack the system and collect the data or go through unauthorized.The most prominent of pandemics cyber virus are

- Mydoom.
- Sobig.
- Klez.
- ILOVEYOU.
- WannaCry.
- Zeus.
- Code Red.
- CryptoLocker.
- Sasser

Once a laughing matter, computer viruses are now a damaging and costly plague on our internet-connected world. More than 350,000 new pieces of malware are discovered every day, with an annual cost of over 55 billion. But one virus – the Mydoom virus in 2004 – leads the pack with 38 billion in damages. This article ranks the most destructive computer viruses by financial impact. But bear in mind that these malicious programs are just the tip of the iceberg. With 127 million new malware apps attacking consumers and businesses each year, the viruses in this article are just the biggest fish in an endless cybercrime sea.[2]

2 Background

The first section, i show how the cyber attack happen on the several site and institution and those attact cause many hampering on hardware and software The Department of Homeland Security (DHS) Federal Network Security (FNS) program created the Risk and Vulnerability Assessment (RVA) program to assist Federal Civilian Executive Branch (FCEB) agencies with conducting risk and vulnerability assessments [1]. These assessments individually identify agency-specific vulnerabilities and combine to provide a view of cyber risk and vulnerability across the entire federal enterprise. The RVA program has worked with Sandia National Laboratories to develop a basis Operational Threat Assessment (OTA) methodology that will result in an unclassified estimate of current threats to an FCEB system to be shared with the system owner [2]. The goal of the OTA phase of a risk and vulnerability assessment is to provide an accurate appraisal of the threat levels faced by a given FCEB agency. Information is collected about the system being assessed through document review and targeted searches of both open source and classified data sets. The identified threats, vulnerabilities, mitigations, and controls may be confirmed or discounted during assessment activities. OTA is designed to provide an efficient threat estimate that is consistent from agency to agency and analyst to analyst. Given the scope of the RVA program, a large number of assessments will be conducted each year, addressing agencies with widely varying sizes and missions. The consistency and repeatability of each threat assessment is important to ensure similar treatment of all agencies and facilitate the combination of risk assessment results for all agencies. Toward this end, this report reviews cyber threat metrics and models that may potentially contribute to the OTA methodology .In might include:

- 2010 January: The Waledac botnet sent spam emails. In February 2010, an international group of security researchers and Microsoft took Waledac down.[58] January: The Psyb0t worm is discovered. It is thought to be unique in that it can infect routers and high-speed modems.[59] February 18: Microsoft announced that a BSoD problem on some Windows machines which was triggered by a batch of Patch Tuesday updates was caused by the Alureon Trojan.[60] June 17: Stuxnet, a Windows Trojan, was detected.[61] It is the first worm to attack SCADA systems.[62] There are suggestions that it was designed to target Iranian nuclear facilities.[63] It uses a valid certificate from Realtek.[64] September 9: The virus, called "here you have" or "VBMania", is a simple

Trojan horse that arrives in the inbox with the odd-but-suggestive subject line "here you have". The body reads "This is The Document I told you about, you can find it Here" or "This is The Free Download Sex Movies, you can find it Here";

- 2011 SpyEye and Zeus merged code is seen.[65] New variants attack mobile phone banking information.[66] Anti-Spyware 2011, a Trojan horse that attacks Windows 9x, 2000, XP, Vista, and Windows 7, posing as an anti-spyware program. It disables security-related processes of anti-virus programs, while also blocking access to the Internet, which prevents updates.[67] Summer 2011: The Morto worm attempts to propagate itself to additional computers via the Microsoft Windows Remote Desktop Protocol (RDP). Morto spreads by forcing infected systems to scan for Windows servers allowing RDP login. Once Morto finds an RDP-accessible system, it attempts to log into a domain or local system account named 'Administrator' using several common passwords.[68] A detailed overview of how the worm works – along with the password dictionary Morto uses – was done by Imperva.[69] July 13: the ZeroAccess rootkit (also known as Sirefef or max++) was discovered. September 1: Duqu is a worm thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab)[70] of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu.[71][72] Duqu gets its name from the prefix " DQ" it gives to the names of files it creates.[73]

- 2012 May: Flame – also known as Flamer, sKyWIper, and Skywiper – a modular computer malware that attacks computers running Microsoft Windows. Used for targeted cyber espionage in Middle Eastern countries. Its discovery was announced on 28 May 2012 by MAHER Center of Iranian National Computer Emergency Response Team (CERT), Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. CrySyS stated in their report that "sKyWIper is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found".[74] August 16: Shamoon is a computer virus designed to target computers running Microsoft Windows in the energy sector. Symantec, Kaspersky Lab, and Seculert announced its discovery on August 16, 2012.

- 2013 September: The CryptoLocker Trojan horse is discovered. CryptoLocker encrypts the files on a user's hard drive, then prompts them to pay a ransom to the developer to receive the decryption key. In the following months, several copycat ransomware Trojans were also discovered. December: The Gameover ZeuS Trojan is discovered. This type of virus steals one's login details on popular Web sites that involve monetary transactions. It works by detecting a login page, then proceeds to inject malicious code into the page, keystroke logging the computer user's details. December: Linux.Darlloz targets the Internet of things and infects routers, security cameras, set-top boxes by exploiting a PHP vulnerability.[77][78]

- 2014 November: The Regin Trojan horse is discovered. Regin is a dropper,

primarily spread via spoofed Web pages. Once installed, it quietly downloads additional malware, making it difficult for signature-based anti-virus programs to detect. It is believed to have been created by the United States and United Kingdom as a tool for espionage and mass surveillance.[citation needed]

- 2015 The BASHLITE malware is leaked leading to a massive spike in DDoS attacks.[79] Linux.Wifatch is revealed to the general public. It is found to attempt to secure devices from other more malicious malware.[80][81][82]
- 2017 May: The WannaCry ransomware attack spreads globally. Exploits revealed in the NSA hacking toolkit leak of late 2016 were used to enable the propagation of the malware.[97] Shortly after the news of the infections broke online, a UK cybersecurity researcher in collaboration with others found and activated a "kill switch" hidden within the ransomware, effectively halting the initial wave of its global propagation.[98] The next day, researchers announced that they had found new variants of the malware without the kill switch.[99] June: The Petya (malware) attack spreads globally affecting Windows systems. Researchers at Symantec reveal that this ransomware uses the EternalBlue exploit, similar to the one used in the WannaCry ransomware attack.[100][101][102] September: The Xafecopy Trojan attacks 47 countries, affecting only Android operating systems. Kaspersky Lab identified it as a malware from the Ubsod family, stealing money through click based WAP billing systems.[103][104] September: A new variety of Remote Access Trojan (RAT), Kedi RAT, is distributed in a Spear Phishing Campaign. The attack targeted Citrix users. The Trojan was able to evade usual system scanners. Kedi Trojan had all the characteristics of a common Remote Access Trojan and it could communicate to its Command and Control center via Gmail using common HTML, HTTP protocols.[105][106]
- 2018 February: Thanatos, a ransomware, becomes the first ransomware program to accept ransom payment in Bitcoin Cash.[107]
- 2019 November: Titanium is an advanced backdoor malware, developed by the PLATINUM APT.[108]
- 2021 July: Journalists and researchers report the discovery of spyware, called Pegasus, developed and distributed by a private company which can and has been used to infect iOS and Android smartphones often – based on 0-day exploits – without the need for any user-interaction or significant clues to the user and then be used to exfiltrate data, track user locations, capture film through its camera, and activate the microphone at any time. The investigation suggests it was used on many targets worldwide and revealed its use for e.g. governments' espionage on journalists, opposition politicians, activists, business people and others.[109]

3 Methods

There are so much mehtod to do cyber attack.With the application of advanced computer and communication technologies, traditional power system has been coupled with communication system and transformed into cyber-physical power system (CPPS) [1]. Through sensor networks and communication networks, CPPS can acquisition real-time operation information of power system. Communication system enhances the observability and controllability of modern power system. But it also makes power systems suffer from possible cyber-attacks [2]–[6]. Some method are describe below:

- A. False Data Injection Attack (FDIA) FDIA is an important kind of cyber-attack which is able todisturb the power system state estimation. The FDIA can makethe state estimator to transfer erroneous values to the systemoperator, leading to undesirable outcomes in power system. State estimation can estimate the current operation state ofpower system based on various measurement information. Theaccuracy of state estimation determines the accuracy ofsubsequent calculation and analysis ;
- B. Denial -of-Service (DoS) Attack DoS attack generally refers to any attacks that make theattacked server fail to provide services properly. Specifically,DoS attack is a destructive mode of attack which consumes theresources of a remote host or network until the system stopsresponding or crashes. And the attacked computers or networks cannot provide normal services to the users [15]. SYN flooding attack and IP spoofing attack are two common forms of a DoS. Limited to length, this paper briefly introduces the principle of SYN flooding attack.
- C. Man-in-the-Middle (MITM) Attack MITM attack is a form of active eavesdropping. It exploits the lack of authentication in a system. The attacker virtually places a computer between two communication computers in a network connection by various technical means. This computer is called “man-in-the-middle”. Then the attacker can pretend to be a legitimate participant, intercepts and manipulates message packets transmitted between two communication computers and injects new message packets without being found. ARP spoofing and DNS spoofing are two common forms.
- spoofing and DNS spoofing are two common forms [16]. 1) ARP Spoofing Address Resolution Protocol is a TCP/IP protocol that gets Ethernet Medium Access Control (MAC) addresses based on IP addresses. The host broadcasts an ARP request containing the target address to all hosts and receives the return messages to determine the target MAC address. After receiving the return messages, the host caches this IP address and MAC address in local ARP cache table and keeps it for a while. The host queries the ARP cache directly on next same request to save resources.
-) DNS Spoofing Domain Name System (DNS) maps domain name and IP address to each other in the form of distributed database. In brief, DNS is

used to resolve domain names. With DNS, the server can be available through relatively simple domain names instead of complex IP addresses. Even if the server changes its IP address, it can still be accessed through the domain name.

- all information is correct; and
- 3) Delay Attack Delay is a version of DoS attack. The attacker can insert delay into the signal transmitted through the communication channel, which affects the stability of power system. Flooding the network with a huge amount of redundant data traffic to consume the target resources such as network bandwidth may cause delay attack. Then the bandwidth for the useful data is limited and the data measured will experience the long communication delay. As a consequence, the system operators would be blinded and the grid vulnerability to further attacks or inappropriate operations increases.
- D. Replay Attack Replay attack is one of the most popular securityattacksbased on interception of a system's usage pattern. Replayattack is mainly used in the process of identity authenticationand destroys the correctness of authentication. Theattackersends a message packet that has been received bythetargethost to spoof the system[17]. The basic principle of replay attack is tosendthepreviously eavesdropped data to the receiver without doinganychange. When the attacker knows the function of thedata, hecan mislead the receiver by sending the data againwithoutknowing the content of the data. For example, whenafaultoccurs in power system, the attacker can send dataduringnormal operation, which makes the operation center mistakethat the system is still in normal operation state, thus delayingthe time of fault processing and expanding the impact of fault.Similarly, when power system is in normal operation, theattacker can send data during the fault operation, whichmaymake the control center issue an erroneous control command.[5]
- E. Other Attacks In addition to the above several typical cyber-attacks, thispaper also summaries some other cyber-attacks whichmayhave adverse effects on the safe and stable operationof powersystem.
- 2. Load Altering Attack LAA is a cyber-physical attack against demandresponse(DR) and demand side management (DSM) programs.
- 3) Delay Attack Delay is a version of DoS attack. The attacker can insert delay into the signal transmitted through the communication channel, which affects the stability of power system. Flooding the network with a huge amount of redundant data traffic to consume the target resources such as network bandwidth may cause delay attack. Then the bandwidth for the useful data is limited and the data measured will experience the long communication delay. As a consequence, the system operators would be blinded and the grid vulnerability to further attacks or inappropriate operations increases .[6]

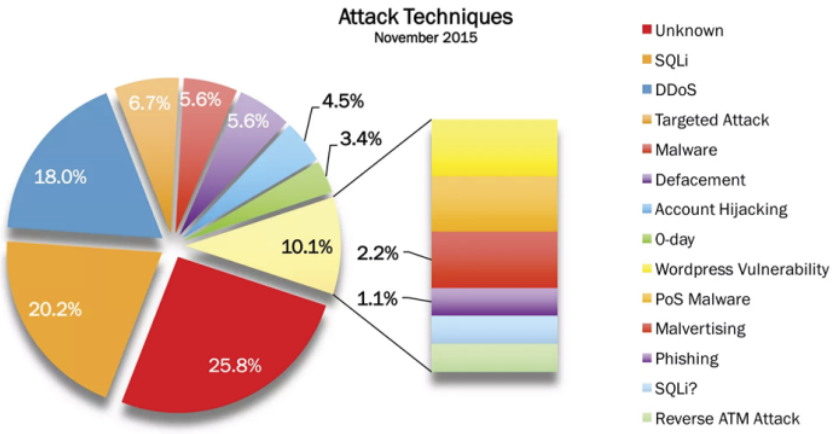

Figure 1: Analysis of attack

4 Results

All those attack which i describe cause many of problem. Cyber-terrorism has been much discussed in the media, especially at times of heightened international tension. The Institute for Security Technology Studies has tracked previous attacks and, using conflicts such as the Israel-Palestine and India-Pakistan as examples, shows there is a strong correlation between political and military conflicts and the incidence of cyber-terrorism. Research group IDC has recently predicted that in the next year we can expect to experience a cyber-terrorist attack as a result of a war on Iraq, resulting in short term economic disruptions. Cyber attacks can

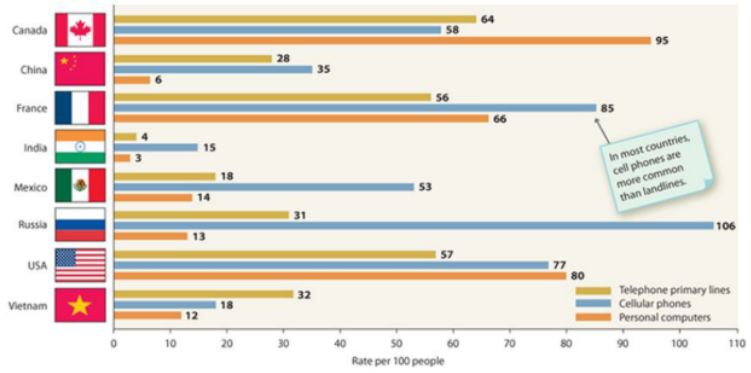

Figure 2: Country graph

cause electrical blackouts, failure of military equipment, and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. he Red Cross has revealed that personal data belonging to

more than half a million "highly vulnerable" people was compromised via the abuse of an unpatched vulnerability.

Nearly a month after detecting and disclosing the intrusion, the International Committee of the Red Cross (ICRC) said on Wednesday (February 16) that its investigation had encountered a "highly sophisticated and targeted" attack.

Attackers had optimized malicious code for ICRC servers and anti-malware defenses, deployed sophisticated obfuscation techniques, and used hacking tools "primarily used by advanced persistent threat groups" in order to "disguise themselves as legitimate users or administrators", said the humanitarian organization. Malicious hackers are targeting Office 365 users with a spare of 'MFA fatigue attacks', bombarding victims with 2FA push notifications to trick them into authenticating their login attempts.

This is according to researchers from GoSecure, who have warned that there is an increase in attacks that are exploiting human behavior to gain access to devices.

Multi-factor authentication (MFA) fatigue is the name given to a technique used by adversaries to flood a user's authentication app with push notifications in the hope they will accept and therefore enable an attacker to gain entry to an account or device.[3] Cyber-weaponry threats 3.1. Stuxnet and the nature of its cyber weaponry

Table 1. Potential Financial Consequences of a Cyber-Attack

Type of Firm	Type of Attack	
	DoS	Security Breach
Conventional Brick and Mortar (e.g., Coca-Cola)	Lowest	
Click and Mortar (e.g., Borders)		
Internet Firms (e.g. Amazon, E-bay)		Highest

Figure 3: Potential Financial Consequences of a Cyber-Attack [1]

Stuxnet is an incredibly large and complex threat that written primarily to target an industrial control system (ICS) or a set of similar systems. Its final goal is to reprogram the ICS by modifying the code on the PLC to make it work in a manner intended by the attacker and to hide any changes from the equipment operator (Falliere et al., 2011). To achieve this objective, the creators amassed a vast array of components to increase likelihood of their success, including zero-day exploits, the Windows rootkit, the first-ever PLC rootkit, antivirus evasion techniques, complex process injections, hooking codes, network infection routines, peerto-peer updates, and a command-and-control interface. 3.2. Attacking possibility of Stuxnet-like malware Since Stuxnet, an attack unprecedented in its sophistication, there have been many cases of weaponized malware, including Duqu, Flame, Gauss, and Shamoon.

These are variants of and/or inspired by Stuxnet and are designed to steal information and destroy industrial control systems. In addition, the source code of Stuxnet was posted on the Web shortly after it was first identified, and therefore the possibility of Stuxnet-inspired malware attacks has increased dramatically. That is, hackers can simply reuse the specific components and technologies available online for their own attacks. Further, the reverse engineering of the binary execution file is possible and can restore the structures and major components of the Stuxnet code, and there are many analysis reports posted online related to Stuxnet, that can be used as reference for its reproduction and modification. This suggests that Stuxnet may serve as a prototype for future generations of cyber attacks. 4. Countermeasures against cyber threats The advancement of plant data networks (PDN) employed in Nuclear Power Plants introduce the potential cyber threats proliferated in IT environments, whereas the PDN improve the efficiency and reliability of the protection, control, and monitoring system resulting in enhancement of overall plant operation. A primary countermeasure for protecting the safety system against malicious cyber threats is the development of a security policy that provides a framework from which plant personnel can identify the important network components, and create a plan to secure network access and its operation (Nuclear Regulatory Commission, 2012). In addition, the monitoring the network is necessary in terms of anomaly and heuristic analysis with network traffics, and the placing the firewall, IDS/IPS security devices within network perimeters. The PLC is most popular hardware devices to implement the instrumentation and control system in NPP. The secure approaches to preventing the potential for malicious programs to be propagated into PLC are (1) ensure that flash update scheme requires an authentication mechanism, (2) provide proper access control to protect firmware images during storage, (3) prohibit remote updates, and disable removable media, such as thumb drives (John et al., 2010). Viruses are self-propagating software that spread from one file to another on a single computer and/or from one computer to another using a variety of methods. Virus is type of malware that is inserted into a system or network. Malware can conceal that the computer system has been compromised, disable security measures, and damage and affect the integrity of the data on the system. The Slammer and Stuxnet are type of worm–virus attacked the Nuclear I and C system, while Duqu, Flame, Gauss and Shamoon attacked the industrial control system (ICS). The important means of protecting a computer system from malware is through code signing that is the process of creating a cryptographic-based digital signature. Another malware protection technique is to apply the software restriction policy.[4]

5 Conclusion

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.Every one need to know the ethics and rule of cyber attack and hardly follow the rule.And make the site more hard to crack and critical more complex.

Acknowledgements

All of this work done for some find some bad effet and malicious work on some site .And i want to find the most dangerous tools for crack site .I have no enough knowledge to implement but idea how to do it .For this case i need some help and some paper that help me much.

A Appendices

Supplier shall ensure all Products have been developed in accordance with principles of secure software development consistent with software development industry best practices, including, security design review, secure coding practices, risk based testing and remediation requirements. Supplier's software development environment used to develop the Products must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk based manner. Supplier must develop and maintain an up-to-date Cybersecurity Vulnerability management plan designed to promptly identify, prevent, investigate, and mitigate any Cybersecurity Vulnerabilities and perform any required recovery actions to remedy the impact.Supplier shall notify Buyer within a reasonable period, in no event to exceed five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability. Supplier shall report any Cybersecurity Vulnerability to Buyer at such contact information communicated to Supplier from time to time. Within a reasonable time thereafter, Supplier shall provide Buyer, free of charge, with any upgrades, updates, releases, maintenance releases and error or bug fixes necessary to remediate any Cybersecurity Vulnerability. Supplier shall reasonably cooperate with Buyer in its investigation of a Cybersecurity Vulnerability, whether discovered by Supplier, Buyer, or a third party, which shall include providing Buyer a detailed description of the Cybersecurity Vulnerability, the remediation plan, and any other information Buyer reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. Buyer or Buyer's agent shall have the right to conduct a cybersecurity assessment of the applicable Products, and the Product development lifecycle, which includes tests intended to identify potential cybersecurity vulnerabilities. Supplier shall designate an individual responsible for management of the Cybersecurity Vulnerability, and shall identify such individual to Buyer promptly.

References

[1] Brian Cashell, William D Jackson, Mark Jickling, and Baird Webel. The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC)*, 2, 2004.

[2] Richard Dawkins. Viruses of the mind. *Dennett and his critics: Demystifying mind*, 13:e27, 1993.

[3] Lech Janczewski and Andrew Colarik. *Cyber warfare and cyber terrorism*. IGI Global, 2007.

[4] Do-Yeon Kim. Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy*, 65:141–143, 2014.

[5] Michael E Kuhl, Moises Sudit, Jason Kistner, and Kevin Costantini. Cyber attack modeling and simulation for network security analysis. In *2007 Winter Simulation Conference*, pages 1180–1188. IEEE, 2007.

[6] Qi Wang, Xingpu Cai, Yi Tang, and Ming Ni. Methods of cyber-attack identification for power systems based on bilateral cyber-physical information. *International Journal of Electrical Power & Energy Systems*, 125:106515, 2021.

Md Raju Biswas

ORIGINALITY REPORT

80%	58%	38%	31%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	en.wikipedia.org Internet Source	23%
2	Feng Li, Xinteng Yan, Yunyun Xie, Zi Sang, Xiaoshu Yuan. "A Review of Cyber-Attack Methods in Cyber-Physical Power System", 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), 2019 Publication	15%
3	Do-Yeon Kim. "Cyber security issues imposed on nuclear power plants", Annals of Nuclear Energy, 2014 Publication	14%
4	mafiadoc.com Internet Source	7%
5	www.gesupplier.com Internet Source	7%
6	www.researchgate.net Internet Source	5%
7	portswigger.net	

	Internet Source	2%
8	v1.overleaf.com Internet Source	2%
9	Submitted to Uganda Technology and Management University Student Paper	2%
10	Submitted to Champlain College Student Paper	1%
11	www.coursehero.com Internet Source	1%
12	www.bitdegree.org Internet Source	1%
13	global.oup.com Internet Source	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Md Raju Biswas

PAGE 1

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Proper Noun If this word is a proper noun, you need to capitalize it.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 3

Proper Noun If this word is a proper noun, you need to capitalize it.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

Proper Noun If this word is a proper noun, you need to capitalize it.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Wrong Form You may have used the wrong form of this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Confused You have used **an** in this sentence. You may need to use **a** instead.

Possessive You may need to use an apostrophe to show possession.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Proper Noun If this word is a proper noun, you need to capitalize it.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without

conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 5

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word. Consider using the article **the**.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Confused You have used **a** in this sentence. You may need to use **an** instead.

Confused You have used **an** in this sentence. You may need to use **a** instead.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

PAGE 6

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

Proper Noun If this word is a proper noun, you need to capitalize it.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Proper Noun If this word is a proper noun, you need to capitalize it.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

Confused You have used **of** in this sentence. You may need to use **have** instead.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Confused You have used **to** in this sentence. You may need to use **two** instead.

PAGE 9

Proper Noun If this word is a proper noun, you need to capitalize it.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to remove this article.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

Sentence Cap. Remember to capitalize the first word of each sentence.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word. Consider using the article **the**.

Possessive You may need to use an apostrophe to show possession.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 10

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

Wrong Form You may have used the wrong form of this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

Proper Noun If this word is a proper noun, you need to capitalize it.

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word.

Coord. Conjunction These sentences begin with coordinating conjunctions. Try to combine them with the sentences that precede them.

Proper Noun If this word is a proper noun, you need to capitalize it.

Confused You have used **A** in this sentence. You may need to use **an** instead.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.