iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 Issue: V Month of publication: May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5150

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Review of Information Security: Issues and Techniques

Aayush Rai[1], Ajay Shanker Singh[2], A. Suresh Kumar[3]
[1, 2, 3]School of Computer Science and Engineering, Galgotias University, Greater Noida, India

Abstract: Currently, companies are more into using distributed systems and relying on network and communication facilities for transmitting critical and important information that needs to be secured. Therefore, protecting companies information becomes more important, and information security is essential to maintain. Information security is defined as protecting the information, the system, and the hardware that use, store and transmit the information, to ensure integrity, confidentiality and availability of data and operation procedures are protected. In this paper, we illustrate the factors that impact information security in different fields; cyber security, Internet of Things and network security from various studies and outline the security requirements to reduce this impact.

Keywords: Information Security, Cyber Security, Network Security, Internet of Things, Attacks

I. INTRODUCTION

Nowadays, most of the companies are interested in technology system in order to achieve a quicker procedure than the old-fashioned way, and for this system to be more effective, it must be saved from threats and information security must be maintained. The main objectives of information security that must be implemented to ensure the protection of data in any corporation are: (i) confidentiality, (ii) integrity and (iii) availability. The companies structure should be protected from active and passive attacks, such as (illegal access, unauthorized improvement of data and interruption) [1]. Information security and cyber security are both global and exciting subject for many researchers. The international standard, ISO/IEC 27002 (2005), defines Information Security as: “The preservations of the confidentiality, integrity and availability of information, for any form (hard copy or soft copy, electronic store, transmitted by email, or any other format)”. While, the International Telecommunications Union (ITU) defines cyber security as follows: “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets” [2]. Both cyber security and information technology security requires continuous assessment and newness because they are vastly developed fields. Reputation and compromise intellectual property of organization will be affected by cyber attacks. Cyber attackers face problems in system security that uses multi-layer firewalls, so they depend on social engineering [3].

Due to the rapid increase of using technologies, that provide some comfort to the user, such as saving time and effort. The Internet of Things (IoT) is considered the best technology, with its applications that facilitate our work and live by providing features (i.e. connectivity, active engagement) that help us to achieve improvement, increase evolution and knowledge exchange. IoT is defined as a group of people and devices interconnected with each other. In addition, it allows devices to communicate with each other without involvement of human, it includes interconnected sensors of real world, devices of electronics and systems to the Internet. The main support of the IoT is the Internet. So that, any security threats that target the Internet can affect the IoT [4].

According to the importance of network and technology for any application, the security of network should be taken very important. The design of network depends on Open System Interface (OSI) model that gives many benefits when designing network security (e.g. flexibility, standardization of protocols, and easy to use). Network is unprotected to attacks while transferring data into communication channels. The security requirements of network are confidentiality and integrity. In addition, it is better to confirm that the complete network is secure when considering with network security [5].

In this paper, we will illustrate the factors effect on the multiple domains (Information System IS, cyber space, IoT and Network security) from various studies, to show how these factors effect and what are security requirements that can be used to reduce this effect. The reminder of this paper is organized as follows. Section II illustrates studies of various topics IS, Cyber space, IoT, and Network. In Section III, we discuss about different attacks that effect on security of multiple fields and the security requirements to prevent the attacks. Section IV is devoted to represent some relevant comments and concluding remarks.

II. RELATED WORK

Information security is considered as an exciting field for researches and many studies were conducted on it. This section will highlight different studies about information system and attacks on many fields of security such as: cyber security, Internet of Things and network security.

A. *Information Security*

Researchers in [2] concerns to define both topics (Information Security, Information and Communication Technology ICT security). Firstly, for information security they defined it by referring to ISO/IEC 27002 and Whitman and Mattord (2009) definitions, then they examined these definitions to show some concepts that relate to information security, which include: Information security is about process not procedure or technology, also they define information security prosperities or characteristics as in confidentiality, integrity and availability (CIA) triangle. Secondly, for information and communication technology security, by exploring some definitions from both ISO/IEC 13335-1 and Dhillon (2007), they define ICT security as the protect of information resource that allocated in information technology system. Finally, they detect that for information to be protected, the communication and technology can be considered a unsafe factor that can be a target to threats.

B. *Cyber Security*

For cyber security threats, authors in [2] investigate some structures to show how the threats can affect cyber space.

Different structures they studied are: (cyber bullying, home automation, digital media and cyber terrorism). Cyberbullying, is considered as a wide cyber security problem that can cause a direct damage to a person who is the goal of this bullying. Home automation application allows home owners to manage different systems like (home security, hot water geysers and televisions, etc.) with web-based management system, that in role can increase risks by unauthorized access to these systems and cause some damages. For digital media, they discuss the impact of illegal sharing of digital media, and how it can be a direct affect to the legal owner by caucusing some financial problems. Critical infrastructures of country can be considered as the goal of cyber terrorist via cyber space, which can cause direct attack (e.g. attack on the national electricity grid) or indirect attack (e.g. denial of service attack). Figure 1 below shows the relationship between Information Security, ICT Security and Cyber Security.

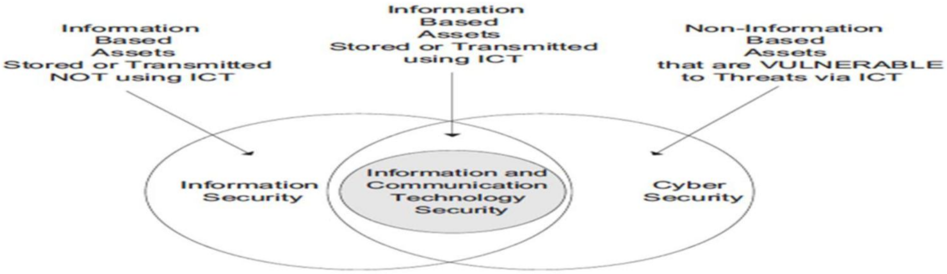

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 1. Information Security, ICT Security and Cyber Security [2]

Authors in [6] explain many recent attacks to the power system. The researchers explain cyber attacks of Cyber Physical Power System (CPPS) as the attacks that effect system power or resources for the purpose of damage. Also, they classify the cyber attack into target based attack and network-based attack. Several attacks for network-based classification (Wide Area Network, Neighborhood Area Network and Home Area Network) and an example of the targets of these attacks (Power Generation Assembly, Power Substation and Home Appliances) respectively. Moreover, according to the target-based attack, the first target could be on confidentiality, which can cause illegal use of data. The second could be on integrity, which causes illegal modification of data. The last target could be on availability, which causes data unavailability. Furthermore, the researchers illustrate different methods to conduct target-based attacks, for example (Brute force password, Man in the Middle and Denial of Service). In addition, the paper investigates three different structure of cyber attack that effect on CPPS from power generation, transmission, distribution and consumption. In [7] authors categorize cyber threats into three various categories, which are (cyber terror, cyber crime and cyber war). In addition, they focus on studying cyber space of India, they also mentioned the major types of cyber attacks, which are: (cyber crime, Hacktivism, cyber espionage and cyber warfare). Also, they show the total percentage of attacks during 2013-1014 is 243 from various attacks. Finally, they showed how India tries to prevent and stop cyber attacks and crime by introducing cyber policies. In 2013, Indian government imports National Cyber Security Policy to provide protection from cyber attacks of both private and public infrastructures.

C. Internet of Things

The network structure of the IoT is divided into three layers: the bottom layer is the sensing equipment for information acquisition; the middle layer is the network for data transmission, while the top layer is designed for applications and middleware, as shown in Figure 2. The overall security requirement of the IoT is in fact an integration of security in physical meaning, information acquisition, information transmission, and information processing, and the ultimate aim of protection is to guarantee the confidentiality, integrality, authenticity, and instantaneity of data and information [8].

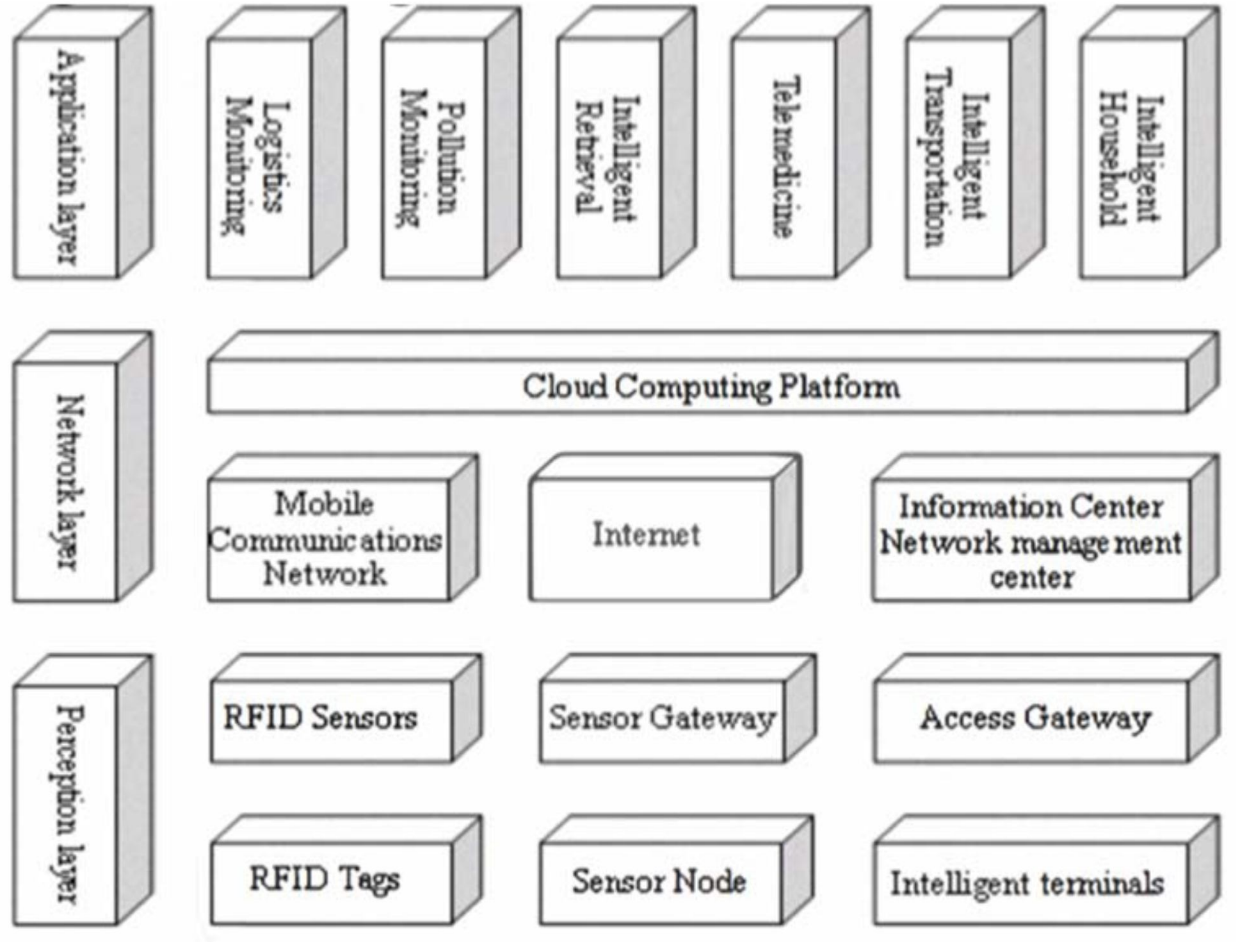


Figure 2. Architecture of the Internet of Things [8]

For IoT attacks, authors in [4] discuss various IoT attacks that work on three layers of IoT system architecture, which are (perception layer, network layer, and application layer). They studied different attacks (Physical Attacks, Network Attacks, Software Attacks, Encryption Attacks) in different layers. Based on the vulnerabilities of layers they classify the attacks in four categories, as shown in Figure 3. From each category, they considered one attack as the most dangerous. From physical attack, malicious node injection attack has been the most terrible attack, since it does not only stop the services, but also modify the data. From network attack, sinkhole attack is the riskiest attack. It is an insider attack where an intruder compromises a node inside the network and launches an attack. Then, the compromised node tries to attract all the traffic from neighbor nodes based on the routing metric that used in routing protocol. From software attack, worm attack is considered as most dangerous attack. Worms are probably the most destructive and dangerous form of malware on the Internet. It is the self-replicating program, which harms the computer by using security holes in networking software and hardware. It can delete the files from the system, steals information (like passwords), and they can also change the passwords without the owner noticing, it also causes the computer lockouts. From encryption attack, side channel attack is the most difficult to handle. It is hard to detect it because an attacker uses the side channel information to perform the attack [4].

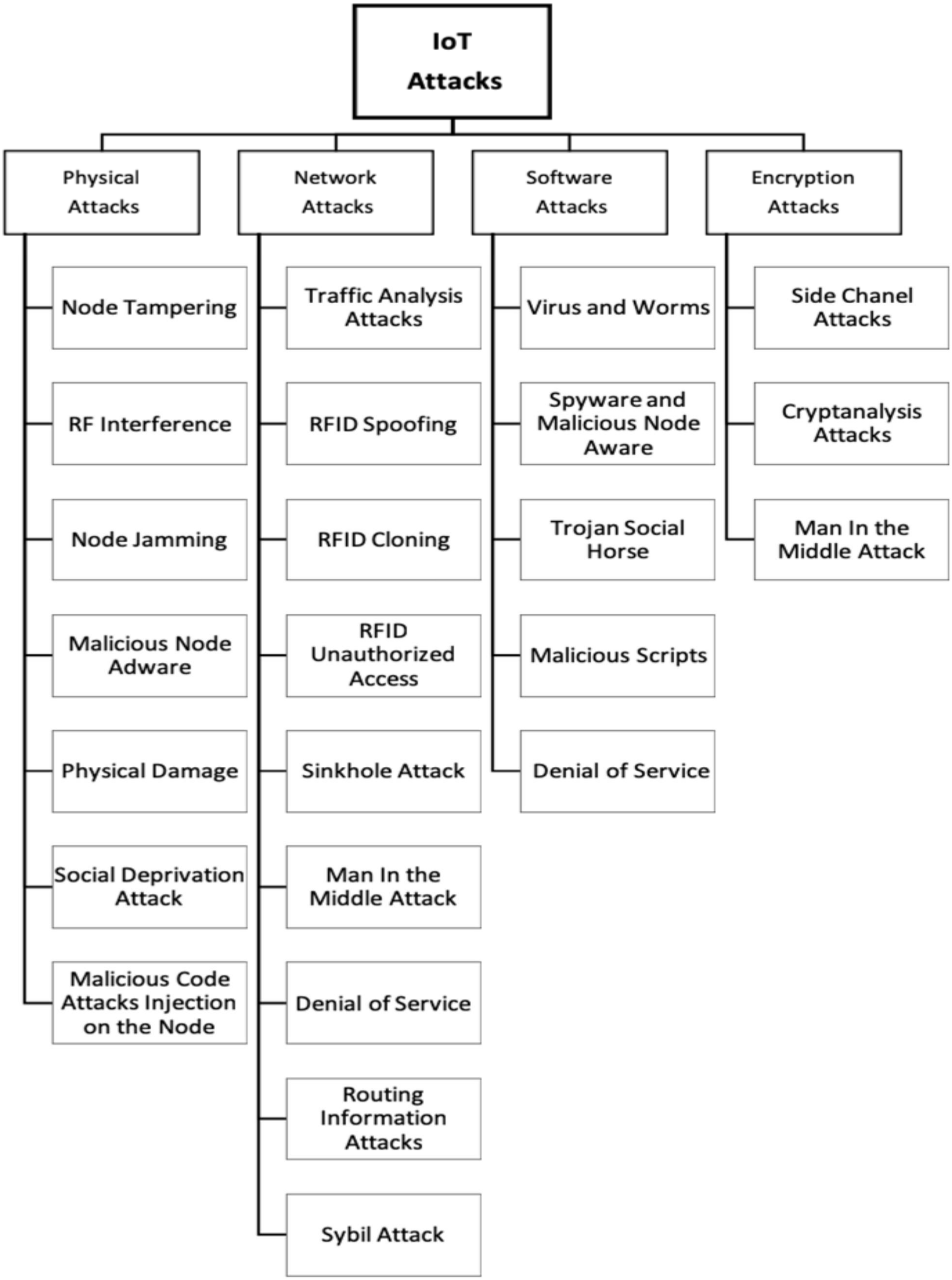
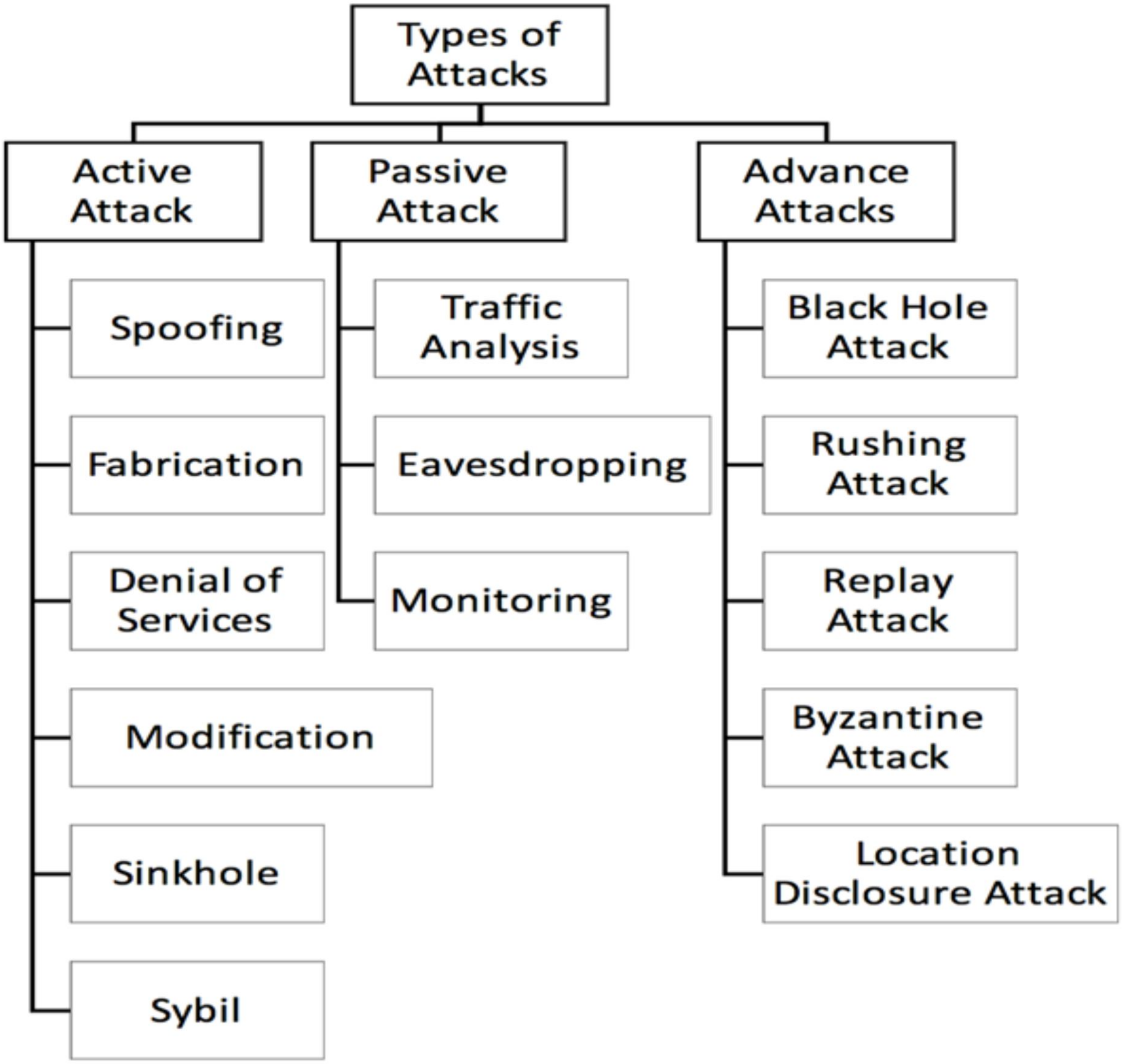


Figure 3. Internet of Things and its security attacks [4]

D. Network Securiy

For network security attacks, authors in [5] categorized some basic class of network attacks in three categories that are illustrated in Figure 4, in addition, they suggest to perform some procedures to avoid security gaps, including regularly updating the operating system, having an updated antivirus program, and limiting the access to any network user.Figure 4. Types of network attacks.



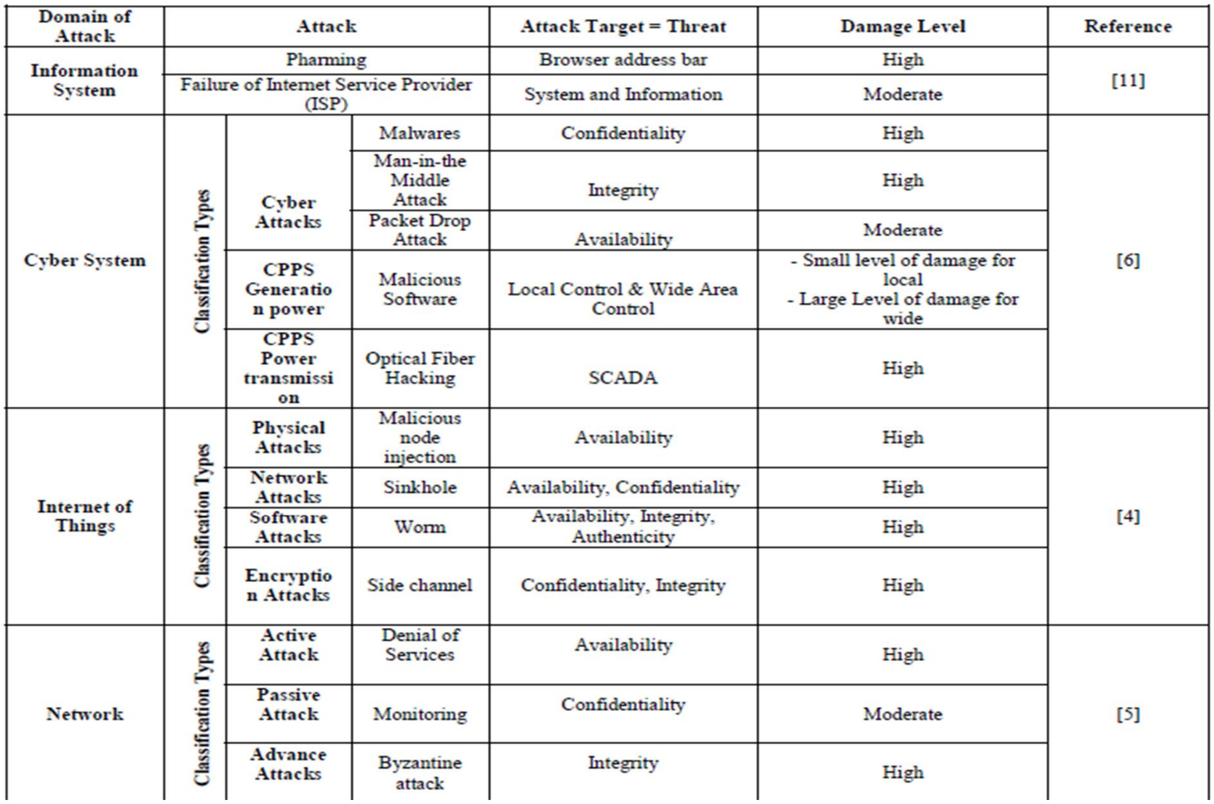
In order to investigate attacks on different systems, authors in [9] made a security analysis of the network communication between the components of SCADA systems namely, Programmable Logic Controllers (PLCs) and the engineering stations, they showed that this communication can be compromised by successfully conducting three network security attacks, replay attack, Man-In-The-Middle attack (MITM), and Stealth command modification attack, these attacks allow to interfere with the PLC-Process Control System 7 (PLC-PCS7) communication and send commands to the PLC that control and reprogram it, this leads to serious SCADA system insecurity.

For exploring a specific attack in [10] the authors who are a group of computer scientists, showed a vulnerability in the popular internet protocol Diffie-Heltlmen by presenting a new attack (Logjam attack) that enables a man-in-the-middle attacker to downgrade vulnerable Transport Layer Security (TLS) connections from 1024-bit to 512-bit export-grade cryptography, which allows the attacker to successfully intercepts communication between two systems. Nowadays, a huge number of servers use weak Diffie-Hellman parameters, applies to 8.4% of Alexa Top Million Hypertext Transfer Protocol Secure (HTTPS) sites and 3.4% of all HTTPS servers that have browser-trusted certificates. Therefore, authors recommend switching to Elliptic Curve Diffie-Hellman (ECDH) key exchange, which with appropriate parameters can avoid all known feasible cryptanalytic attacks.

III. DISCUSSION

We compare some attacks from specific domains, by considering various properties such as damage level and attack threat. The comparison is summarized in Table I

TABLE I. COMPARISON OF DIFFERENT ATTACKS



Domain of Attack	Attack			Attack Target = Threat	Damage Level	Reference
Information System	Pharming			Browser address bar	High	[11]
	Failure of Internet Service Provider (ISP)			System and Information	Moderate	
Cyber System	Classification Types	Cyber Attacks	Malwares	Confidentiality	High	[6]
			Man-in-the Middle Attack	Integrity	High	
			Packet Drop Attack	Availability	Moderate	
		CPPS Generation power	Malicious Software	Local Control & Wide Area Control	- Small level of damage for local - Large Level of damage for wide	
		CPPS Power transmission	Optical Fiber Hacking	SCADA	High	
Internet of Things	Classification Types	Physical Attacks	Malicious node injection	Availability	High	[4]
		Network Attacks	Sinkhole	Availability, Confidentiality	High	
		Software Attacks	Worm	Availability, Integrity, Authenticity	High	
		Encryption Attacks	Side channel	Confidentiality, Integrity	High	
Network	Classification Types	Active Attack	Denial of Services	Availability	High	[5]
		Passive Attack	Monitoring	Confidentiality	Moderate	
		Advance Attacks	Byzantine attack	Integrity	High	

A. *Information, Cyber, IoT, Network Attacks*

Attacks on both information system and cyber system can effect the system requirements, which are confidentiality, integrity and availability. Firstly, different information of system attacks discussed in [11], 12 various threat categories are listed (Compromises to Intellectual Property, Deviations in Quality of Service, Espionage or Trespass, Forces of Nature, Human Error or Failure, Social Engineering ,Information Extortion, Sabotage or Vandalism, Software Attacks, Technical Hardware Failures or Errors, Technical Software Failures or Errors, Theft, Technological Obsolescence). In addition, the statistics of some affected attacks were shown (e.g. 2 million of systems was damaged by My Doom malware as well as $38 billions of financial damage). Secondly, for cyber system, number of attacks and scenarios are identified in [7], authors in this article explore attacks on cyber space as general, and they identify some scenarios of specific attacks on CPPS. Thirdly, for attacks that effect on the protocols within the IoT environment. The attacks in this domain is involved in the previous table, including the physical layer which is targeted for malicious node injection attack as the node is physically injected into the network. While sinkhole attack is done at network layer as in this attack routing information is attracted to the node, which has the lowest distance to the base station. The worm attack is performed at the application layer by inserting malicious code, and side channel attack is performed at both application layer and physical layer, because the attacker uses the side channel information emitted by the encryption device. All these attacks result in severe damage as they modify the data, drop the packets, steal private information and encryption key, etc. The malicious node injection attack uses hidden node vulnerability whereas in sinkhole attack, node authentication is not provided. People do not follow security policies such as accessing infected sites or files, spam e-mails, outdated antivirus [4]. Finally, attacks on the network security as illustrated in Figure 4, can be categorized into passive attack and active attack, passive attack in which a network intruder intercepts the data that travels through the network, and active attack where an intruder initiates commands to disrupt the network's normal operation [5].

B. Security Requirements

In order to enhance security solutions in the information system, authors in [11], define guidelines of information security, which are publication of Secure Software Assurance (SSA) and Common Body of Knowledge (CBK), from U.S. Department of Defense and Department of Homeland Security. While security solutions provided for cyber system defined in [7], authors investigate cyber security procedures of Indian government, which are: Indian Computer Emergency Response Team, National Informatics Centre (NIC) and National Information Security Assurance Program (NISAP). In addition, they provide some recommendations for cyber security: (1) Conduct policy of security and assurance. (2) Malicious software should be detected and stopped as soon as possible. (3) Provide various programs and security exercises such as workshops. (4) Improvements of cyber security skills

by conducting (meetings, research works and sessions). Furthermore, like any other networks (e.g., wireless sensor networks), the following general security requirements are essential to secure an IoT network: (Authentication, Integrity, Confidentiality, Availability, Non-repudiation, Authorization, Freshness). Apart from the above security requirements, the following two important security properties should be alsosatisfied:

□□Forward secrecy: when an IoT sensing node quits the network, any future messages after its exit must be prohibited.

□□Backward secrecy: when a new IoT sensing node is added in the network, it it must be stopped from reading any previously transmitted message [12]. Network security is the main concern of today's generation of computing as many types of attacks are growing day by day. Securing the Network includes protecting the system objects, which are either tangible or nontangible from both internal and external unauthorized access and modification, the tangible objects are the system hardware resources, and th intangible object are the information and data in the system, in both transition and static in storage. Protecting hardware resources include protecting:(1) End user objects including user interface hardware components (mouse, keyboard, touchscreen, etc.). (2) Network objects (switches, firewalls, routers, gateways, hubs, etc.). (3) Network communication channels to prevent observers from intercepting network communications. Protecting software resources includes protecting hardware-based software, operating systems, browsers, server protocols, etc. Prevention of unauthorized access to the resources is accomplished through several services (access control, authentication, confidentiality, integrity, and nonrepudiation). Several security protocols and standards are used for security and privacy in electronic communication, among these are Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, secure Internet Protocol (IPsec), Secure Hypertext Transfer Protocol (SHTTP), secure e-mail (Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME)), Secure Shell (SSH), and others as summarized in Table II.

[13]. Table II. (Application, Transport, and Network) Layer Security Protocols and Standard

TCP/IP	ISO	Security Protocols
Application	Application/Presentation	RADIUS, TACAS, PGP, S/MIME, S-HTTP, HTTPS, SET, SSH, and
		KERBEROS
Transport	Session/Transport	SSL and TLS
Network	Network	IPsec, VPN, PPTP and L2TP

paper explored a review of information security, cyber security, network security, and IoT security. Moreover, we demonstrated the main factors that impact on them from various studies. Also, we defined the security requirements to prevent the attacks on multiple fields. The security is not necessarily confined to the protection of cyberspace, IS, Network or IoT, but it also includes the protection of those who function and any of their assets.

This study can be extended by developing some tools that would increase the security related to one of the four fields (information system, cyber space, IoT and network). In addition, Machine Learning Algorithms can be used to find best security solutions or to define the impact of some attacks.

REFERENCES

[1] F. Alqahtani, "Developing an Information Security Policy: A Case Study Approach", *Procedia Computer Science*, vol. 124, pp. 691-697, 2017.

[2] R. von Solms and J. van Niekerk, "From information security to cyber security", *Computers & Security*, vol. 38, pp. 97-102, 2013.

[3] R. Torten, C. Reaiche and S. Boyle, "The impact of security awarness on information technology professionals' behavior", *Computers & Security*, vol. 79, pp. 68-79, 2018.

[4] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey", in *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 32-36.

[5] M. Pawar and J. Anuradha, "Network Security and Types of Attacks in Network", *Procedia Computer Science*, vol. 48, pp. 503-506, 2015.

[6] Yi Tang, Qian Chen, Mengya Li, Qi Wang, "Challenge and Evolution of Cyber Attacks in Cyber Physical Power System", in *PES Asia-Pacific Power and Energy Conference*. IEEE, 2016, pp. 857-862.

[7] Shipra Ravi Kumar, Suman Avdhesh Yadav, Smita Sharma, Akansha Singh. "Recommendations for Effective Cyber Security Execution". In *1st International Conference on Innovation and Challenges in Cyber Security*, pp. 342-346, 2016.

[8] L. Li, "Study on security architecture in the Internet of Things", In *Proceedings of 2012 International Conference on Measurement, Information and Control*. IEEE, 2012, pp. 375.

[9] A. Ghaleb, S. Zhioua and A. Almulhem, "On PLC network security", *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 62-69, 2018.

[10] ADRIAN, D., BHARGAVAN, K "Imperfect forward secrecy: How Diffie-Hellman fails in practice". In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 5– 17, 2015.

[11] M. Whitman and H. Mattord, *Principles of information security*, pp. 39- 82, 5th ed.

[12] A. Das, S. Zeadally and D. He, "Taxonomy and analysis of security protocols for Internet of Things", *Future Generation Computer Systems*, vol. 89, pp. 110-125, 2018.

[13] J. Kizza, *Guide to Computer Network Security*, 4th ed. Springer, 2017, pp. 44-47,367,381,385.