Importance of Cyber security and its sub-domains

Tanvir Fatima Naik Bukht*[1], Mubasher H. Malik[2], Rizwan Ahmad[3], Shahab ud din umer[4]

[1]*Institute of Southern Punjab, Multan, Pakistan*

[2]*Departmemt of Computer Science, Institute of Southern Punjab Multan*
[3]*Riphah International University, Lahore, Pakistan*
[4]*Federal Urdu University of Arts, Science & Technology Islamabad, Pakistan*
[1]*fatimaishtiaq7@gmail.com,* [2] *mubasher@isp.edu.pk,* [3]*rk640841@gmail.com*
[4]*Shahabuddinumer@gmail.com*

Abstract

Cyber attacks are becoming smarter and more dangerous as our need for information technology increases. The protection of data, systems, Information, and application has become one of the main tasks. That's why it's really important to understand about cyber security. Data protection and data security will always be the most important security features that every organization deals with. We are currently living in a global world where the facts are kept in a digital or cyber form. Due to advancementof ICT (Information and communications technology) and cyberage, various numbers of privacy and security challenges have been identified and reported. Hence, a new field is extended in cyber world titles as Cyber-security. In this paper, we provide an overview of the cybersecurity and its subdomains or its functions also explains the Major areas of cyber security.

Keywords: Cyber security, Network security, Domains of Cyber-security, Cyber-Physical system.

1. Introduction

Cyber security is method, process and techniques which involved protecting data, information, computer system, software applications and networks from cyber-attackers. Currently, cyber-attacks have become even more complicated and advanced [1]. Our society, economy, and important infrastructures must rely heavily on their networks and IT solutions. A report was found bu computer crime and security analysis that malware was injected, computer theft, phishing and bot attacks were carried out on the basis of common cyber attack concepts to obtain sensitive material, causing damage to the organization. [2]. The increasing no of cyber-attacks on digital technology and communication networks attracted the attention of ICT professionals, cyber security wings and other security officials to enhance the security level.

Cyber security is a very imperative part of the cyber world. Because cyber security is a method of defending information, software, network, and facts from unauthorized access or attacks. Cyber safety performs an essential function within the area of statistics technology. Securing the information, network, records, and the application has come to be one of the largest challenges. Cyber security is a very important part of the cyber world. Because cyber security is a performance of protecting data, application, system, and information from illegal access or attacks._Cyber security shows a necessary part in the arena of information technology. Cybersecurity covers the physical and non-physical security of data against internal and external attacks or threats. The physical attack can damage hardware, software, and sensitive data or information. Non-physical threats such as viruses and piracy come from illegal access to the system[3]. While the physical domain includes hardware, software and networks as a structure block of cyber substructure [4].

2. Domains of Cybersecurity

The field of cybersecurity is categorized into main six domains are as follows Cyber-Physical domain, Information domain, Network domain, Cognitive domain, Social domain, and Transportation domain.

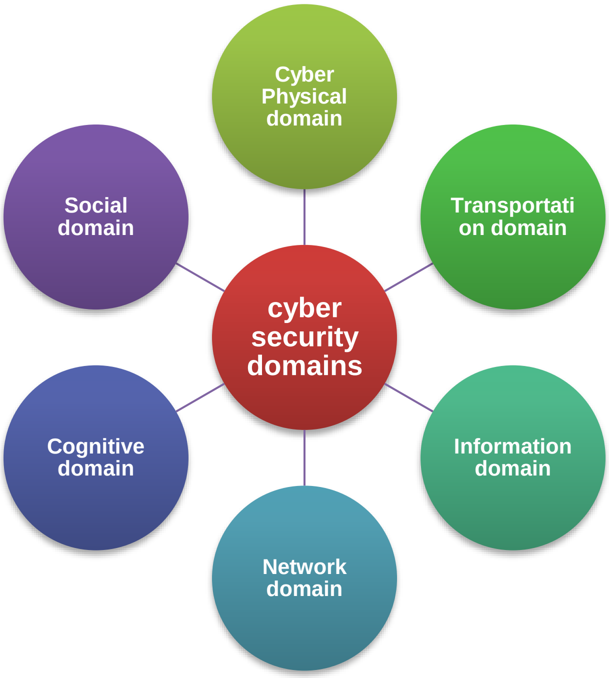
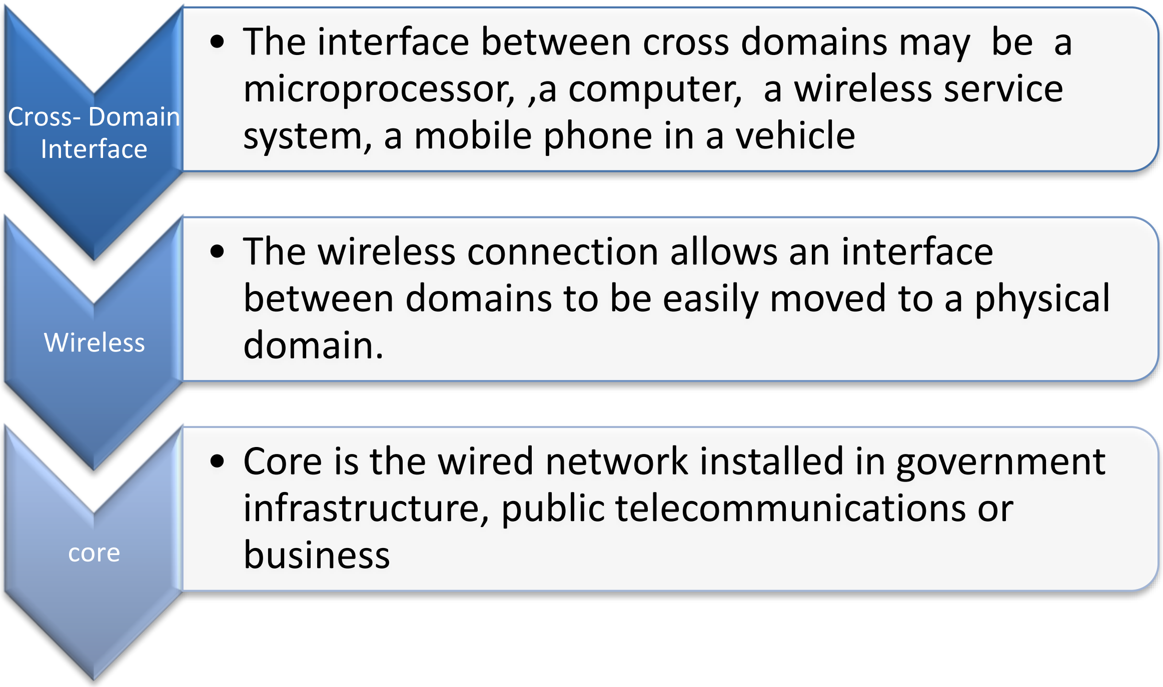


Figure 1. Cybersecurity domains

2.1 Cyber-Physical domain

The physical domain is an essential part or subdomain of cybersecurity. Information technology infrastructure work as a medium in the physical domain used to transfer information. The cable Internet connection is formed as the core of the cyber domain. The interface between domains is the endpoint in the cybersecurity domain. The wireless layer accepted a cross-domain limit to easily transition to a physical domain. Currently, research is focused on the cross-domain interface and the central layers of the cybersecurity domain [5].



- The interface between cross domains may be a microprocessor, ,a computer, a wireless service system, a mobile phone in a vehicle
- The wireless connection allows an interface between domains to be easily moved to a physical domain.
- Core is the wired network installed in government infrastructure, public telecommunications or business

Figure 2. Three functional layers of the cyber Physical domain

The physical cyber domain consists of three functional layers from a technical point of view. The first part is Core, the second part is Wireless and the Third part is the layer cross-domain interface[5]. Core Layer offer tracks to a discussion of data and network information between different subnets[6].

In the cyber-physical system, two methods of data collection are used for an audit of material such as Host base audit and Network-based audit. A host-based audit is preferred for the system with a high volume structure such as the smart grid. The network-based audit has a benefit in freeing each node from maintaining or analyzing logs [1][7], [8]. Basic network computers for example switches, load balancers, routers, and firewalls can capture network traffic they are going through. which is generally considered to be the main source of control data for intrusion detection [9]. The two most popular categories of data sources such as the host base and network base, this designing an anomaly-based data source: calls, UNIX, shell commands, mouse, dynamic, keyboard, multiple host records, users. The hosts are valid [9]. Host-based IDS is not a good solution for fast dispersion worms without dispersion [10]. The most common examples of a network-based data source are Network traffic and records [9]. The IDE-based network is located at strategic points in the system and controls all movement between devices. The host-based IDE runs on distinct hosts on the network and controls the internal and outbound traffic of these particular devices[11]. The host-based model notifies the cloud user of malicious activity in the system by analyzing the tracking of system calls [12]. The CPS ranges from comparatively small systems such as airplanes and cars to large systems such as a national network [13]. The cyber-physical system is a system for observing and controlling the physical world. The Cyber system used in various applications, such as military, medical assistance, transportation, and production. Four representative applications used in CPS, such as business control systems, smart grid systems, medical/health devices and intelligent vehicles[14]. Programmable judgment managers are replaced by the advanced cyber physics system (CPS). In general, CPS communicates through a closed industrial communication network and also links to the Internet. The PSC monitors the physical processes that are integrated devices for free programming and attacks on cyber systems can cause physical damage and threaten human life [15]. The intelligent network has become one of the main technological and economic developments in the world [16]. Medical devices have been improved by integrating physical and cybersecurity capabilities to provide better health services[17]. Smart cars (smart cars) are more environmentally friendly and safer cars [14]. CPS attacks can not only have financial implications, but they can also endanger people's lives. Therefore, the security of the CPS is important. [18].

The traditional CPS system involves in many vast industrial projects such as the manufactory system, the smart electric power grid, aerospace system, protection system, aerospace system and so on. Mobile CPS services can be useful in numerous application domains mostly introduced in three application fields, healthcare system, vehicular networking system, and mobile education. Healthcare systems have been an energetic research area. The healthcare system in traditional CPS more likely about live sport medical devices and robot-supported operation etc. Vehicular networking system divided into three groups, microlayer, macro layer, and meso layer. Data handling and transmissions are complex in vehicular networking systems. Micro layer is used for traffic security, traffic awareness, or in many other operations. Meso layer is about communication among different vehicles and shares security information. Macro layer useful in real-time traffic information [7].

2.2 Information domain and its features

Cybersecurity is the same as information security. Information security is part of cybersecurity [19]. The exchange of information on situational awareness is extremely crucial for an organization that allows it to continue to exist as part of the cybersecurity domain. Knowledge of the condition is essential for decision-making and a timely threat to future threats. Due to the confidential nature of information, there is always a risk that security information will be shared. [20].

The characteristics of the information domain are the monitoring, archiving, and display of information. In the information domain, there are many issues like simulation-based risk, management based risk, risk on traffic control systems [4]. Information security awareness training is a formal education for computer users who know information security. Training at the workplace is usually a rule that motivates the behavior of information security [2]. The class's material can be characterized in a different type of classifier such as Artificial neural network, Rule induction, Decision tree, Bayesian method, evolutionary algorithms, and K Nearest neighbors, etc. [8].

2.3 Network domain and its security

The network domain also shows a very central role in exchange and communication. The security of a system/network is one of the most important components for the protection of private data. Most attackers try to access and take control of any internal system, as taking advantage of one system facilitates control over other systems in the network [21]. Network security consists of hardware and software methods to avoid security breaches and provide security measures. However, IT support implements security measures such as the use of firewalls and antivirus protection in an organizational context [2].

The security of the network domain is also required as the usage of the networks increases day by day. Other data and information are generated. Real-time defense of information and data is becoming increasingly difficult for today's businesses. DDoS (Distributed Denial of Service) attacks are commonplace today [21], [22]. Trojans of the Denial of Service (DoS) prevent the functioning of a function or source [23]. If enterprise security requirements are not very high, we can take the protection of by-hop encryption. Or, if the demands on commercial requirements are high, we can use end-to-end cryptography [24]. Attacks on industrial systems are often recognized as machine learning since K represents the clustering, the neural network, the intelligent Markov mode based on statistical learning, and the classification of the supporting machine[25]. The K-means clustering algorithm is often used in intrusion detection. However, the algorithm is sensitive to selecting the center of the original group[26]. Many methods for detecting intrusions and protecting the network from attacks, such as detection of abuse or detection based on the comprehensive signature protocol (SPA) based detection anomalies and the hybrid system[1], [8], [21]. Intrusion detection is an area of impotent investigation. Many devices are available to detect intrusion in the network [8]. Based on the understanding of attack detection, we also introduce block-chain technology and its main application. The simple functionality of a block-chain is a cryptographically secure mechanism for finding a verifiable sequence of data records [1]. Cryptography is divided into two symmetric and asymmetric categories. The symmetric cryptographic algorithm works in sequence and used to transform data in privacy, for example, the advanced encryption standard (AES). Transport keys and digital signatures used in an asymmetric cryptographic algorithms.[24].

Security and network information should be treated with such characteristics as integrity, identification, non-refusal, and confidentiality [24].

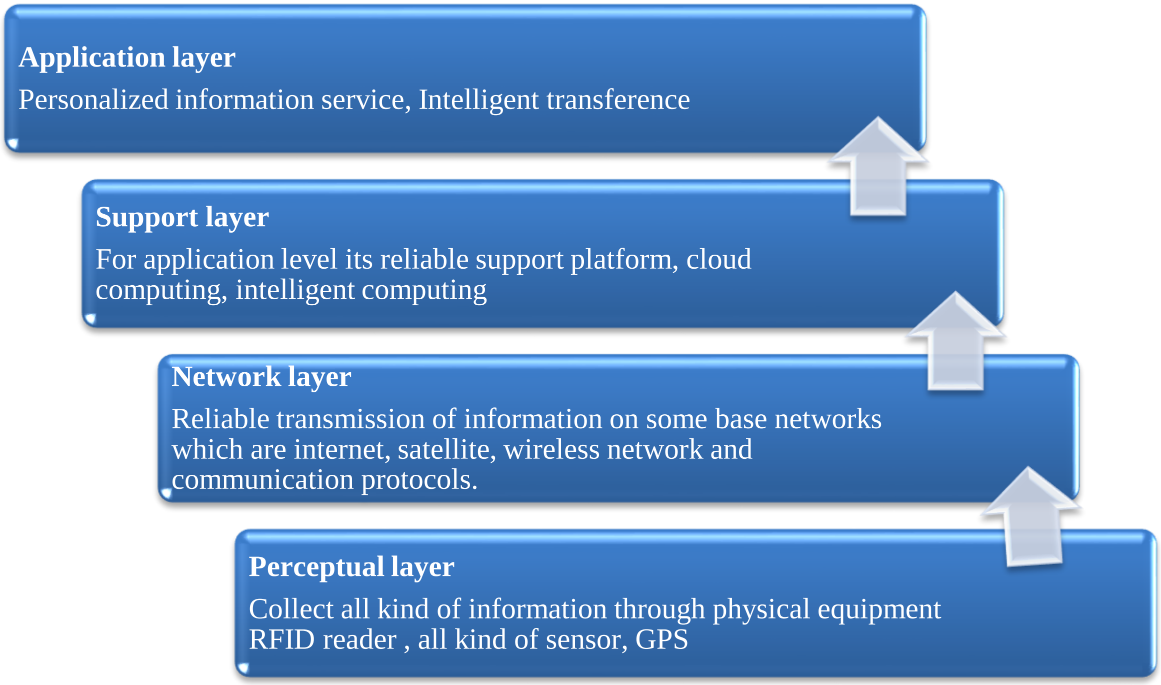

Application layer
Personalized information service, Intelligent transference
Support layer
For application level its reliable support platform, cloud computing, intelligent computing
Network layer
Reliable transmission of information on some base networks which are internet, satellite, wireless network and communication protocols.
Perceptual layer
Collect all kind of information through physical equipment RFID reader , all kind of sensor, GPS

Figure 3. Network Security Architecture

Figure No 3, shows four key levels of network security. It is shared into four main levels, with the most basic level being the level of awareness, the second level the network level, the third level the support level, and the last level the application level [24].

The perception level collects information about physical devices. The level of the network is in control for the consistent transmission of information on certain core networks such as the satellite, Internet, wireless network; etc. The support level combines the level of the application upwards and the network downwards. This level is a support platform for the application level. Application-level that provides customized installations based on user needs. Verification is more important for security to avoid the illegal node [24].

2.4 Cognitive domain

In the cognitive domain, data needs to be analyzed, accurately recognized, and used for an executive. Pay attention to the cognitive decisions that users make when faced with a computer security problem. Z-Wave is widely used in commercial environments because the Z-Wave protocol for low power wireless communication is widely used in home automation network remote control. Application control in smart homes and small businesses [27]. The heuristic of intelligent decision making that people apply to a computer security problem. They show the impact of experiments where the scope of loss of utility has become a change for individuals when presented in cybersecurity scenarios [4].

2.5 Social domain

The social domain in cybersecurity is also important for decisions, the perspective of the organization; Describe how organizations prepared to respond to cybersecurity threats can be improved. Decisions on cybersecurity must be reliable with social, moral, and other considerations that are representative of its surrounding social environment[4]. Social networking sites are very useful for the new generation and their very preferred method of communication. Each of the social networking sites generally provides tools for users to share their personal information, photos, and stories. Attackers use social networks and social networks to steal personal information for fraud and identity theft [23]. Since most of them use social networking sites or social almost every day, it has become a great platform for cybercriminals to hack personal data and steal valuable records[28].

2.6 Transportation domain

In the transport domain, the application level offers the facilities demanded by the client and Provides high-quality intelligent services to meet client needs. The intelligent transport system (ITS) or the cyber transport system represents the integration between information technology and communication to monitor and control the transport network. ITS aims to improve the reliability, availability, safety, and efficiency of transport infrastructures[27]. Safety plays an important role in modern cybersecurity systems (CPS), which contain intelligent transport systems. Ad hoc vehicle networks are at the heart of intelligent transport systems (ITS). Its goal is to communicate competently and provide benefits to people, ranging from improved security to accessibility[29].

Table 1. shows the purpose and function of cybersecurity domains.

S.No	Domain Name	Purpose or function
1	**Cyber-Physical domain**	Cyber-Physical domain used to protect hardware, software, and important data or information. The cyber-physical system used in several applications such as health care, military, transport, and industrialized.
2	**Information domain**	Information security domain awareness exercise is correct teaching targeted at making computer user alert of information security. Information domain is used for monitoring, information storing, and conception.
3	**Network domain**	Network domain used in sharing and communication. The network is one of the most important parts of protecting private records. The network must be ready with these properties, such as integrity, identification, non-rejection, and privacy.
4	**Cognitive domain**	The information must be properly analyzed and recognized and used in the field of cognitive decision-making. Cognitive domain, which is widely used in remote control applications in smart homes as well as in small commercial domains.
5	**Social domain**	The social domain in cybersecurity is important for assessments, executive side. Provide awareness on how organizations can be improved arranged to react to cyber threats. Protect data from cybercriminals who try to hack personal information.
6	**Transportation domain**	The transportation domain provides extraordinary quality or smart services to meet the customer’s requirement. The Intelligent transportation system ITS goals to improved reliability, accessibility, safety and efficacy of the transportation infrastructure.

3. Major areas of cybersecurity

Some important areas of cybersecurity are as follows

3.1 Application security

Using the software for many purposes, the user can use the software to protect their business needs. Any application can also contain gaps or vulnerabilities that allow attackers to infiltrate consumer software. Application security is the use of hardware, software, and methods to protect against external pressures. The security processes included in application security programs and software minimize the possibility that administrative applications may access, steal, modify, or delete unauthorized code on a security tool [30].

3.2 Information security

Information security is a set of techniques for managing the processes and tools required to prevent, and handle threats to policies for digital and non-digital documents[31]. Privacy issues are based on intermediate goals such as maintaining integrity, confidentiality, and availability of IT systems and the originality of information. Confidentiality means that confidential data must be disclosed to authorized events, integrity that prevents unauthorized modification of records and availability ensures that information is accessed through the legal parties when required[30].

3.3 Email security

Email security is the number one threat address for a security hole[30]. The email hacking, where hackers can easily access a person's email address and then use it for negative purposes [32]. Attackers use personal information to create sophisticated phishing processes that trick recipients and send them to sites that assign malware. An e-mail security application can block incoming viruses, attack and monitor messages to prevent the loss of private data [30].

3.4 Mobile devices and Web security

Cybercriminals are increasingly focusing on mobile devices and applications. Over the next 3 years, 90% of IT agencies could also support business programs on non-public mobile devices. Obviously, customers want to manipulate which devices can access their network. You may also need to configure your connections to keep visitors to the community site private [30]. Web security protects access to the website or in the cloud. It also refers to the phases in which you defend your website [30].

3.5 Network Security

Network security is used in both hardware and software methods to protect security it also analyses security and security measures [2]. Network security sometimes termed as Wireless security because of an existing network, which becomes wireless and provides access via Access Points. While the wired network is more secure than a wireless network. That’s why; wireless network security is also an emerging issue. Without stringent security features, putting in a wireless LAN may be like putting Ethernet ports anywhere, consisting of the parking zone. To prevent make the most from taking preserve, the consumer needs products particularly designed to protect a wireless network [30].

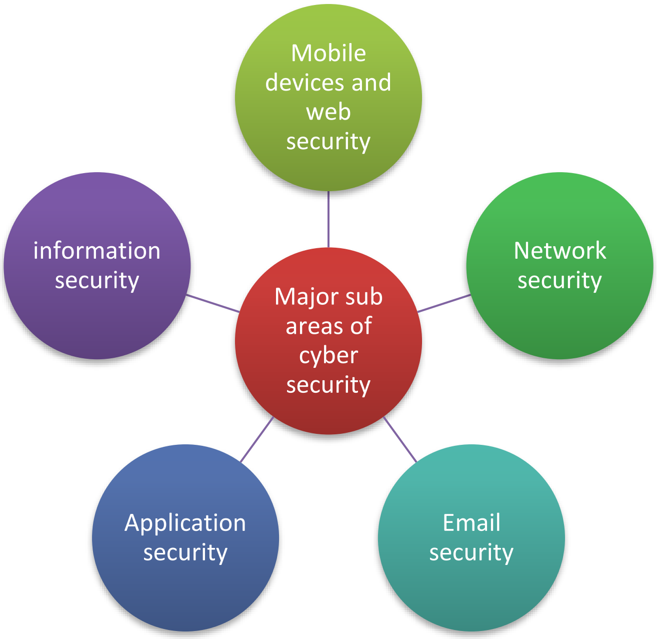


Figure 4. Subareas of cybersecurity

Conclusion

Internet has become an important part of everyone's life. It is widely used in homes, offices, schools, hospitals, and businesses. It is a tool that lets you keep track of things, stay up-to-date with news, and communicate with everyone. In the warfare against cyber-attacks, cybersecurity is a delicate problem in the world of security companies and governments experiencing every effort to deploy or implement various tools and techniques to protect their data and private information in order to keep their business running. It is very important to understand about the usage of cybersecurity domains as security of a system/network is one of the most significant components for the protection of private data. In this paper, we discussed the importance of cybersecurity and usage of its subdomains or its purposes. We also clarify the Major areas of cybersecurity that are most required to avoid and handle threats for digital and non-digital documents.

References

[1] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," IEEE Access, vol. 6, pp. 10179–10188, 2018.

[2] J. Omidosu and J. Ophoff, "A theory-based review of information security behavior in the organization and home context," Proc. - 2016 3rd Int. Conf. Adv. Comput. Commun. Eng. ICACCE 2016, pp. 225–231, 2017.

[3] E. M. O. Abu-Taieh, "Cyber Security Body of Knowledge," 2017 IEEE 7th Int. Symp.

Cloud Serv. Comput., pp. 104–111, 2017.

[4] Z. A. Collier, I. Linkov, and J. H. Lambert, "Four domains of cybersecurity: A risk-based systems approach to cyber decisions," Environ. Syst. Decis., vol. 33, no. 4, pp. 469–470, 2013.

[5] R. D. Whitty, T. O. W. Iii, C. R. Anderson, and S. Member, "Defining the Cyber Domain for Wireless Communications Security," 2011.

[6] H. He et al., "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," in 2016 IEEE Congress on Evolutionary Computation, CEC 2016, 2016, pp. 1015–1021.

[7] Y. Guo, X. Hu, B. Hu, J. Cheng, M. Zhou, and R. Y. K. Kwok, "Mobile Cyber Physical Systems: Current Challenges and Future Networking Applications," IEEE Access, vol. XX, no. c, 2017.

[8] R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," 2017 Int. Conf. Electr. Electron. Commun. Comput. Optim. Tech., pp. 141–147, 2017.

[9] L. Liu, O. De Vel, Q. L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," IEEE Commun. Surv. Tutorials, no. c, pp. 1–21, 2018.

[10] N. Moustafa, J. Hu, and J. Slay, "A holistic review of Network Anomaly Detection Systems: A comprehensive survey," J. Netw. Comput. Appl., vol. 128, pp. 33–55, 2019.

[11] P. Nespoli, D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," IEEE Commun. Surv. Tutorials, no. c, 2017.

[12] P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, "HIDS: A host based intrusion detection system for cloud computing environment," Int. J. Syst. Assur. Eng. Manag., vol. 9, no. 3, pp. 567–576, 2018.

[13] J. Wan, H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, vol. 5, no. 11. pp. 1891–1908, 2011.

[14] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security #x2014;A Survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1802–1831, 2017.

[15] Sadeghi, Ahmad-Reza, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," Annu. Des. Autom. Conf., p. 54, 2015.

[16] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," IET

Cyber-Physical Syst. Theory Appl., vol. 1, no. 1, pp. 13–27, 2016.

[17] J. H. Awan, S. A. Memon, N. A. Memon, R. Shah, Z. Bhutto, and R. A. Bhatti, "Conceptual Model for WWBAN (Wearable Wireless Body Area Network)," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 1, pp. 377–381, 2017.

[18] V. Gokarn, V. Kulkarni, and P. Singh, "Enhancing cyber physical system security via anomaly detection using behaviour analysis," 2017 Int. Conf. Wirel. Commun. Signal Process. Netw., pp. 944–948, 2017.

[19] F. Authors, "Information & Computer Security Article information : Cyber Security and Information Security – What goes where ?," 2017.

[20] T. Kokkonen, J. Hautamaki, J. Siltanen, and T. Hamalainen, "Model for sharing the information of cyber security situation awareness between organizations," 2016 23rd Int. Conf. Telecommun., pp. 1–5, 2016.

[21] R. M. Yousufi, P. Lalwani, and M. B. Potdar, "A network-based intrusion detection and prevention system with multi-mode counteractions," Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017, vol. 2018-Janua, pp. 1–6, 2018.

[22] V. P. Mishra and B. Shukla, "Development of Simulator for Intrusion Detection System to Detect and Alarm the DDoS Attacks," pp. 1–4, 2017.

[23] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, 2014.

[24] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.

[25] H. Yang, T. Chen, X. Guo, X. Wang, and F. Li, "Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm," 2017 IEEE 2nd Inf. Technol. Networking, Electron. Autom. Control Conf., pp. 957–961, 2017.

[26] X. Wang and L. Wang, "Research on Intrusion Detection Based on Feature Extraction of Autoencoder and the Improved K-Means Algorithm," 2017 10th Int. Symp. Comput. Intell. Des., pp. 352–356, 2017.

[27] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[28] G. N. Reddy and G. J. U. Reddy, "A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies," p. 5.

[29] C. Ponikwar and H.-J. Hof, "Overview on Security Approaches in Intelligent Transportation Systems," 2015.

[30] P. R. P. Jitendra Jain, "A Recent Study over Cyber Security and its Elements," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3, pp. 2015–2017, 2017.

[31] J. H. Awan, S. Memon, M. Shah, and F. H. Awan, "Security of eGovernment Services and Challenges in Pakistan," in SAI Computing, 2016, pp. 1082–1085.

[32] S. Rasool, "Cyber security threat in Pakistan : causes Challenges and way forward," Int. Sci. Online J., vol. 12, pp. 21–34, 2015.