AN EFFICIENT CYBER SECURITY USING CYBER DATA ENCRYPTION SECURITY ALGORITHM FOR COMMUNICATION

Dr.BUCIO PITTY Assistant Professor

East Point college of Engineering and Technology .

Dr.S.BELWIN JOEL Assistant Professor

CSE, East Point college of Engineering & Technology

Dr.REGAN MOODY, Assistant Professor

CSE, College of applied Science(IHRD), Thamarasser

Abstract

Today, to ensure the security and reliable online communication of information between organizations, it is essential to maintain a high-security level. However, security and other network data communication on the Internet are always under the threat of intrusion and unauthorized use.Data leakage is from a safety database, or unauthorized warehouse hacking or potential data information steals.The attack of viruses and hackers, more aggressive, has been a need for a better way to protect the communication network has become more technical.The proposed Cyber Data Encryption Security (CDES) algorithm based on cybersecurity is used to protect the information and detect malicious attacks and hackers to resolve this problem.Cybersecurity is stored in the confidentiality, integrity website, computer systems, or compromises their individual data communication information through the Internet on computer attack availability and detects the malicious attack.Therefore, the proposed CDES based cybersecurity intrusion detection system has become an important computer and network communication security element.The proposed CDES algorithm is authorized to encrypt the data and generate the secret key for another user to decrypt the information using generated secret key. The proposed Cyber Data Encryption Security (CDES) effectively detects intrusion presentations of various network intrusion detection systems. CDES parameters and evolution were reviewed and detailed implementation. This method uses the information to detect the network attack and hacker through the communication data of evolution and reduce complexity.

Keywords: Cyber security,online communication, Cyber Data Encryption Security (CDES), attack, hacker, computer network.

1. Introduction

Cyber security system described, data and network protection network in the world, all the businesses violated. The rapid advance development of computer internet technology has provided important data information sharing leading to the recent threat and the introduction of organizational data and organizational efficiency.Data cybersecurity for internet users, organizations, and the military has become more important. With the advent of the Internet, the history of safeguards and security has become a major concern, and we can better understand security technology's emergence. The structure itself of the Internet enables many security threats.The modified network architecture can reduce the likelihood of an attack can be sent over the network. May know how to apply the appropriate security attacks. Many companies from the Internet through a firewall and encryption security mechanisms themselves. It develops to help businesses connect to the Internet and protect their information could threaten.

Generally, the intruder or hacker, the system is defined program or as an individual attempt, and succeeded in performing an action that is not allowed by the intrusion or law to the information system. The integrity of computer resources, confidentiality, or please refer to one of the actions set to the expense of availability.The detection operation that undermines the integrity, confidentiality, or availability of computer resources may be called intrusion detection. Intrusion detection systems and equipment monitor malicious activities or policy violations from the network and system activity reporting software application.The entire field of computer cybersecurity is in the stage of vast and evolution. The proposed range covers a brief history that can be traced back starting point's current developments point and the Internet's network security. The direction of the current proposed, the Internet, is to understand the vulnerability because of the background knowledge of the Internet of the attack and the security technology.

The world is becoming more and more Internet interconnection with new network technologies. Personal, commercial, military, and government a lot of information depends on the infrastructure network worldwide. Because it can easily be obtained via the Internet, network security has become a fundamental intellectual property right.An effective network security plan is cyber datasecurity is prevented the potential data information, security needs, and the network to the attacks has been developed to understand the vulnerable factors.There can reduce network computer vulnerability's many products—encryption of the proposed

authentication mechanisms, intrusion detection, security management, and a firewall. Enterprise or internet users use a combination of these tools throughout the world.

Both the Internet and a local area network become more vulnerable to users' mobility in various complex attacks, terms of terminology, and not only the point of changing the services provided. In recent years it has been expanding at an alarming rate.The convenience of the new cyber security technology has brought us to benefit; the computer system is exposed to security threats and complexity. The particular importance is the rapid adoption of new network cybersecurity policies detection, response, the ability to attack as quickly as possible.There is also abnormal based on the type and intrusion detection systems of the two major misuse detection. The misuse detection system is the most widely used and will not detect the intruder in a known pattern. The proposed are used to identify an attack, the source address, destination address, source port, the payload of the destination port, and the communication, as several keywords, made from various network fields.

2. Related Work

Network cybersecurity simulation provides insight into the organization's Anti-threats and large-scale, complex network environment is a beneficial and practical method. From the host to the micro behavior of malicious software on the macro effects of Distributed Denial of Service (DDoS) attacks, various phenomena can be observed, and the use of simulation scenarios analysis [1].Live virtual and construction platforms for cyber security simulation have been developed to support different simulation scenarios and model fidelity levels. , Live virtual, and construction: Many of the platforms for cyber security simulation has been developed to support the simulation scenarios and models in different fidelity level [2].

Cybersecurity is becoming a priority for media companies. A security infrastructure requires careful planning and configuration, considering the security components required for the design [3]. From the countries tile consultants' experience, some basic security features are particularly desirable, connected to the media technology products, Internet Protocol network.These existing characteristics, based on the supplier's recommendations, can also describe the product evaluation, security, and typical large organization security requirements or both network media systems. It has been chosen as a practical improvement to meet the specific requirements [4].

With online cybersecurity and attack detection, artificial intelligence-based algorithms can come up with better results in some cases than the traditional intrusion detection systems

leading role [5]. Evaluation of different characteristics, sophisticated machine pitch algorithm, generally applies to intrusion and detection system.The online network security data set classification is divided into several groups, and it is the first consideration of a group of records [6]. Using this segmentation, according to a set of data, the object of this work, the neural network model (multilayer or relapse), determines activation function. The learning algorithm yields a precision value.

Prototype-based virtual private network intelligence communications switch allows cross-platform artificial intelligence algorithms to identify and classify attacks by traffic logs risk analysis system self-learning mode [7].The platform, disaster recovery, data migration, and risk detection are suitable to ensure virtualization communication between nodes. To test the Artificial Intelligence (AI) algorithm was evaluated as the accuracy of the model for detection and classification risk, some of the cyber-attacks were simulated [8].

Network security forecast events: There is no doubt that that is believed to have the potential to promote an active network's resilience. In recent years, to learn by promoting large-scale network security incidents related to public data and high-profile examples of proactive forecasting cyber threats against changing mainly in response to detecting witnessed the transformation [9]. Simultaneously, government, corporate, and individual Internet users, preparation of the fight to do, and the ability to recover from cyber threats and incidents to improve cyber resilience show more public appetite [10].

An integrated safety device honeypot has sufficient flexibility to allow general network and laboratory courses while supporting network security education [11]. The existing also provides a detailed analysis of the two honeypot architecture.One of them will provide a very opportunity to existing defines and cybersecurity attacks at a low cost [12] [13]. It was developed as a stand-alone device that can be safely integrated into a more complex laboratory environment.The main contribution of the author is to design and implement school physical network labs. The configurable platform, as a small, low-cost, "lightweight" process performance.

In the data increase the development of network technology and Industrial Control System (ICS), network security has become a challenge for the ICS [14] [15]. Risk assessment of dynamic network security plays an important role in the security protection of the ICS network.However, it is difficult to establish an ICS risk propagation model due to insufficient historical data. In this article, the Fuzzy Probability Bayesian Network (FPBN)

method proposed dynamic risk assessment. First, FPBN has been set up to analyze and predict the spread of network security risks [16].

It introduced a mathematical framework of the time of the elasticity of the network security [17]. The guard's purpose is to select the optimum combination of security control to resist the maximum number of attacks. The budget has some of the multi in this organization possible to install anattack level [18].The mathematical model is a Markov chain with the safe state, all possible attacks (attack each state represents a random attack graph), intermediate state, and the successful attack state.

3. Materials and Methods

With the development of the rapid Internet technology of computer networks, people are more aware of the importance of network security.Network security is a major computational problem because many types of attacks are increasing, and protect computers and the network is an important issue.A set of network attacks come from destruction or unauthorized access technology. The proposed CDES algorithm is based on cybersecurity designed to protect computers, networks, program processes, and data.

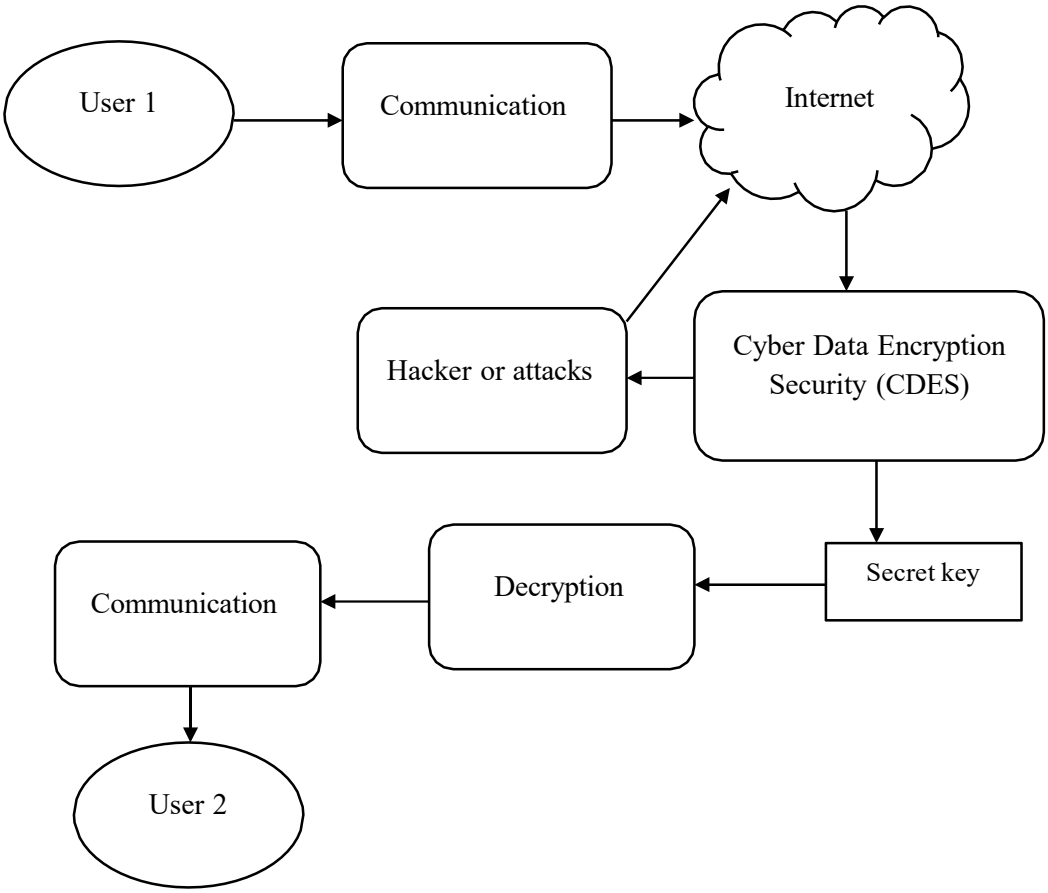

Figure 1: Proposed diagram for cyber security

Figure 1 describes the proposed diagram for cyber security using Cyber Data Encryption Security (CDES) algorithm to detect unauthorized access and attacks. User1 communicates the user2 through the Internet. When a malicious attack steals users the information, the proposed detect the attack and safely send it to authorized users. The proposed algorithm checks the authorized person or not.

3.1 Attacks

The attack is a specific technique that exploits the vulnerability. For example, it may threaten denial-of-service vulnerability as a design of the operating system, and the attack might be a steal of the user's information. There are two categories of attacks there are, passive and active. Passive attacks are difficult to detect because there can be monitored or detected no significant activity. The passive attacks are information eavesdropping and attack analysis, and the Active attacks, as the name implies, use multiple public actions on the network or system.

3.2 Attack and hacker detection using Cyber Data Encryption Security (CDES)

Cyber security, such as the cyber threats from hardware, software, and data, is the Internet protecting the connected systems. The approach uses individuals and companies to prevent unauthorized access to data communication and other computer systems.The proposed Cyber Data Encryption Security (CDES) algorithm protects communication information and detects malicious attacks and hackers. The proposed CDES algorithm is authorized to encrypt the data and generate the secret key for another cyber security user.A set of network attacks come from destruction or unauthorized access technology and are designed to protect computers, networks, program processes, and data.

Algorithm steps

Begin

Step 1: Users can access communication through the Internet

Step 2: If hackers or attack tries to access the information from the Internet

Step 3: Here, the proposed CDES algorithm Generate the secret key for encrypting the information

Step 4: CDES algorithm protect the information and network security from the hacker and attack

Step 5: Using the generated secret key, other authorized users can decrypt the original information and access the information.

Step 6: Thus, the result is succeeded

Stop

The algorithm steps encrypt information for meaningless using the cyber security-based Cyber Data Encryption Security (CDES) algorithm to detect the attackers or hackers. It acts as the mediator between authorized users for communication.

3.3 Secret key Generation

The secret key generation is the most important process of cybersecurity for encrypting the user's information. Secret key encryption uses the same key, encrypted plaintext, and ciphertext decryption.Secret key cryptography, a method that requires the secret key's initial exchange, and symmetric encryption use a single key for encryption and decryption for secure communication between two parties.Encryption such as sending the data, confidentiality, data integrity, and identity has been used to achieve several goals.The proposed algorithm intruder data transmitted from the protection cannot be read ciphertext encrypted message.

3.4 Decryption process

Decryption is a user communication process that includes understanding another receiver user to return the encrypted data to its original form using a secret key. To remove the key from the ciphertext, to generate the same dedicated position on the receiver side, the encryption as described in part) encrypted by the sender, and decryption and the beginning of connection establishment the same process.Authentication user to ensure communications entity to be true. It must be able to find its origin to the recipient of the message using a secret key.The proposed guarantee is undeniable that the recipient can prove that the designated party sent the information. Similarly, the message sender can be proved by a designated recipient.

4. Result and discussion

Cyber security is privacy, and data security is always all organizations take care of best security measures need to be a. All of the information will be stored in the communication through an online form.Cybersecurity has played an important role in the field of information technology. Protect information has become one of the biggest challenges facing today. The proposed using encrypt the data for the security process.

Table 1: Details of simulation parameters

Parameters	**Values**
Simulation language	C#
Simulation tool	Visual studio
Method	CDES
Processor	Intel Core I7

Table 1 shows the details of simulation parameters proposed implementation process the proposed Cyber Data Encryption Security (CDES) algorithm, compared with existing methods are Genetic Algorithm (GA) andFuzzy Probability Bayesian Network (FPBN) algorithm.

Table 2: Examination of cyber security performance

No of transaction	GA in %	FPBN in %	CDESin %
10	70	72	78
20	60	63	83
30	59	52	90
40	47	48	96

Table 2 defines cyber security performance;the proposed algorithm provides high-performance results compared with existing methods.

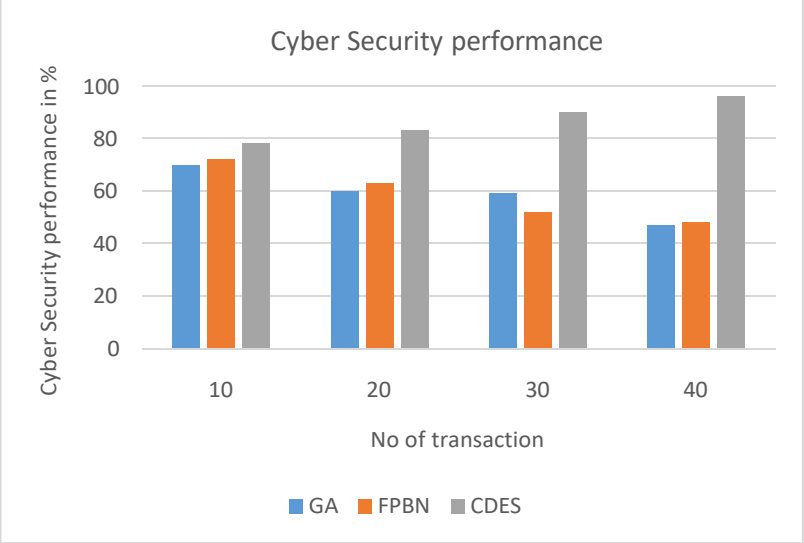

Figure 2: Examination of Cyber Security performance

Figure 2 defines the examination of cyber security performance for secure communicationbetween two parties. The proposed Cyber Data Encryption Security (CDES)algorithm providesa cyber-security performance result is 96%; likewise, the existing method Genetic Algorithm (GA) cyber security performance result is 47%, and Fuzzy Probability Bayesian Network (FPBN) cyber security performance result is 48%.

Table 3:Examination of cyber security throughput performance

No of Transaction	GA in %	FPBN in %	CDES in %
10	66	70	75
20	59	62	82
30	50	54	89
40	42	46	95

Table 3 defines the examination of cyber security throughput performance; the proposed Cyber Data Encryption Security (CDES)algorithm providesa high performance compared with previous algorithms.

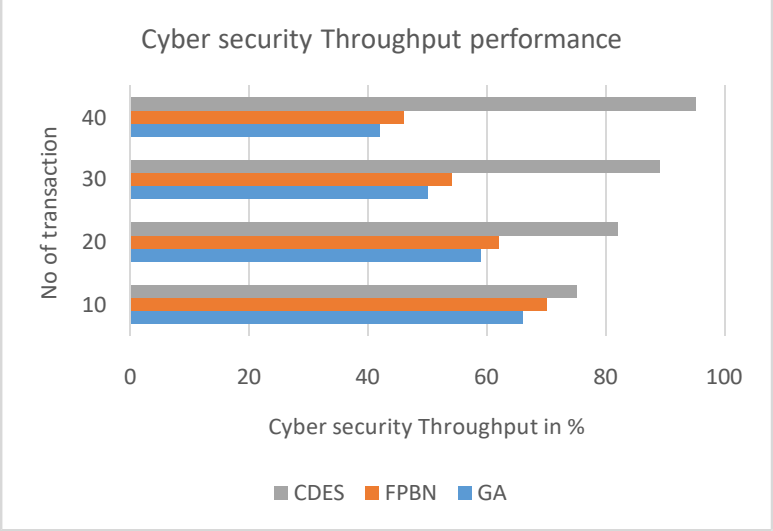

Figure 3:Examination of Cyber security Throughput performance

Figure 3 defines the examination of throughput performance for secure encryption performance. The Proposed Cyber Data Encryption Security (CDES) algorithm throughput performance 95%, Fuzzy Probability Bayesian Network (FPBN)throughput performance result is 46%, and Genetic Algorithm (GA)throughput performance result is 42%.

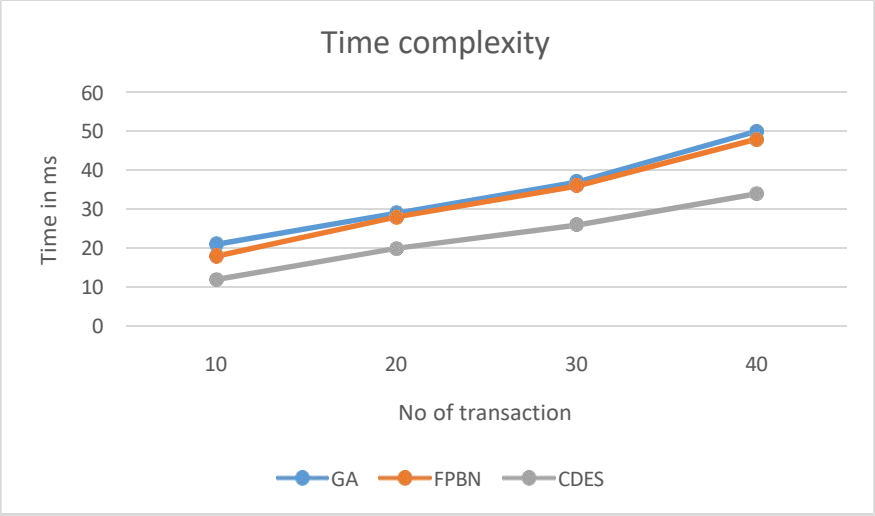

Figure 4: Examination of Time complexity

Figure 4 defines the examination of the time complexity process of cyber security encryption. The proposed Cyber Data Encryption Security (CDES) algorithm time complexity results in34 sec, likewise Genetic Algorithm (GA)algorithm time complexity result is 50 ms, and Fuzzy Probability Bayesian Network (FPBN) time complexity result is 48 ms.

5. Conclusion

An effective cyber security plan is a data is prevented the potential data information, security needs, and the network to the attacks detection has been developed to understand the vulnerable factors.Cybersecurity based on the proposed Cyber Data Encryption Security (CDES) algorithm can help prevent network attacks, data leakage, and personal information theft and assist in risk management. If an organization on safety and effective emergency response plan networks of a strong sense of responsibility can better prevent these attacks, it is serious.The proposed CDES algorithm for encryption and decryption systems of encrypted data provides enhanced assurance levels. An unauthorized person cannot be seen in theft, loss, or intercepted, and Information Security has been used to improve data safety.The proposed CDES algorithm is used for information encrypting by generating the secret key and protect information from hackers and attack an authorized user for meaningless information is then decrypted by using the generated secret key the information of another authorized user for reading format. The proposed Cyber Data Encryption Security (CDES)algorithm provides the result that the security performance result is 96%, throughput performance is 95%, and time complexity result is 34 sec.

References

1. D. Lee, D. Kim, M. K. Ahn, W. Jang and W. Lee, "Cy-Through: Toward a Cybersecurity Simulation for Supporting Live, Virtual, and Constructive Interoperability," in IEEE Access, vol. 9, pp. 10041-10053, 2021, doi: 10.1109/ACCESS.2021.3051072.
2. W. Hooper, "Cybersecurity for Media Technology Products," in SMPTE Motion Imaging Journal, vol. 126, no. 1, pp. 1-4, Jan.-Feb. 2017, doi: 10.5594/JMI.2016.2632358.
3. X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagrá and M. Sanz Rodrigo, "Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies," in IEEE Access, vol. 8, pp. 9005-9014, 2020, doi: 10.1109/ACCESS.2019.2963407.
4. Massaro, M. Gargaro, G. Dipierro, A. M. Galiano and S. Buonopane, "Prototype Cross-Platform Oriented on Cybersecurity, Virtual Connectivity, Big Data and Artificial Intelligence Control," in IEEE Access, vol. 8, pp. 197939-197954, 2020, doi: 10.1109/ACCESS.2020.3034399.

5. N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang and Y. Xiang, "Data-Driven Cybersecurity Incident Prediction: A Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1744-1772, Secondquarter 2019, doi: 10.1109/COMST.2018.2885561.
6. K. Demertzis and L. Iliadis, "A bio-inspired hybrid artificial intelligence framework for cyber security," in Computation, Cryptography, and Network Security. Cham, Switzerland: Springer, 2015, pp. 161–193.
7. N. Eliot, D. Kendall and M. Brockway, "A Flexible Laboratory Environment Supporting Honeypot Deployment for Teaching Real-World Cybersecurity Skills," in IEEE Access, vol. 6, pp. 34884-34895, 2018, doi: 10.1109/ACCESS.2018.2850839.
8. Q. Zhang, C. Zhou, Y. Tian, N. Xiong, Y. Qin and B. Hu, "A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2497-2506, June 2018, doi: 10.1109/TII.2017.2768998.
9. Y. Qin, Y. Peng, K. Huang, C. Zhou and Y. Tian, "Association Analysis-Based Cybersecurity Risk Assessment for Industrial Control Systems," in IEEE Systems Journal, doi: 10.1109/JSYST.2020.3010977.
10. D. Fraunholz, D. Krohmer, S. D. Anton, and H. D. Schotten, "Investigation of cybercrime conducted by abusing weak or default passwords with a medium interaction honeypot," in 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), June 2017, pp. 1–7.
11. Y. Zhang and P. Malacaria, "Optimization-Time Analysis for Cybersecurity," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2021.3055981.
12. J. Díaz, J. E. Pérez, M. A. Lopez-Peña, G. A. Mena and A. Yagüe, "Self-Service Cybersecurity Monitoring as Enabler for DevSecOps," in IEEE Access, vol. 7, pp. 100283-100295, 2019, doi: 10.1109/ACCESS.2019.2930000.
13. U. Adhikari, T. Morris and S. Pan, "WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining," in IEEE Transactions on Smart Grid, vol. 8, no. 6, pp. 2744-2753, Nov. 2017, doi: 10.1109/TSG.2016.2537210.
14. N. Eliot, D. Kendall and M. Brockway, "A Flexible Laboratory Environment Supporting Honeypot Deployment for Teaching Real-World Cybersecurity Skills," in IEEE Access, vol. 6, pp. 34884-34895, 2018, doi: 10.1109/ACCESS.2018.2850839.

15. Angelogianni, I. Politis, F. Mohammadi and C. Xenakis, "On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats," in IEEE Access, vol. 8, pp. 224677-224701, 2020, doi: 10.1109/ACCESS.2020.3045322.
16. P. Mahesh et al., "A Survey of Cybersecurity of Digital Manufacturing," in Proceedings of the IEEE, doi: 10.1109/JPROC.2020.3032074.
17. A. Ali and M. M. Afzal, "Database Security: Threats and Solutions," Int. J. Eng. Invent., vol. 6, no. 2, pp. 25–27, 2017. [Online]. Available: http://www.ijeijournal.com/papers/Vol.6-Iss.2/D06022527.pdf.
18. D. B. Rawat, R. Doku and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2019.2907247.