IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 10, October 2022

DOI: 10.17148/IJARCCE.2022.111008

Securing IoT and NN-based Control Systems Using AI Managed Cybersecurity Techniques in Heavy Industries-A Review

Smrutirekha Panda[1]

Government College of Engineering, Keonjhar, Odisha India[1]

Abstract: In the fourth industrial revolution, all industries are installing sensor-based equipment for better manageability and performance. All these sensors continuously transmit the data and are monitored mainly by neural network-based smart systems. Due to a lack of proper knowledge, utilizing all available resources to maintain the complexity of the operation in securing the control systems is very challenging. Making decisions using traditional technology and software is more difficult to safeguard information against security threats successfully. This paper provides an overview of the artificial intelligence and cyber security implementation prospects in securing IoT-based control systems in the heavy equipment industry. Securing essential information is a concern in today's organizations. Also, this research gave an important reason for securing Neural Network (NN) information in an organization and the benefits and methods used. The study recommends and concludes steps the organization should implement for securing the IoT and NN-based devices also indicate that the organization should contain backup for retrieving information based on the organization's competency.

Keywords: Industry 4.0**,** IoT, sensors, heavy equipment, AI, NN, Cybersecurity

I. INTRODUCTION

Internet of Things (IoT) based control systems in any organizational setup face serious security threats; therefore, only keen technology must be introduced to encounter such threats. IoT is becoming more universal in the modern world, and security flaws must be implemented to protect vulnerable networks and define ways to deter hackers. At the same time, many heavy equipment/control systems are enabled with AI devices for auto-correction and auto-manage. Still, the common problem with these devices is the encrypted data coming from the training data, which interferes with the module, so security and privacy are compromised. In this paper, proper research was conducted about AI-based neural networks' threats and how artificial intelligence and cyber security have safeguarded the confidentiality of information (Dash & Ansari, 2022). Cyber incidents are hazardous most to Network-centric welfare; therefore, cyber defense alterations such as using artificial intelligence techniques and increased cyber security enable the management to boost the organization's confidentiality.

II. BACKGROUND INFORMATION

Artificial intelligence is the intelligence possessed by machines that are beyond human intelligence. A neural network is a sequence of algorithms that focuses on identifying the underlying connection in a group of data via a process that compares to the function of the human brain. Artificial intelligence and cybersecurity provide the best security to IoT-enabled devices for data protection (Ahmed & Diedrich, 2020). Artificial intelligence protects neural networks by removing noise or unwanted information to ensure security experts comprehend the entire cyber environment to identify and address any abnormal activity or behavior. On the other hand, cybersecurity is the implementation of procedures, technologies, and regulations to guard systems, devices, programs, and networks against cyberattacks (Khalid et al., 2019). The concept of cybersecurity was developed in the 1940s. However, since its development, cybersecurity has evolved to become what is currently known as cybersecurity. Due to technological advancement, as cybersecurity evolves, criminal and bad players intending to abuse the system's weaknesses also develop. Since the 1950s, there has been stiff competition between cyber-attacks and security remedies to improve security within the system (Hatfield, 2018). The main aim of developing cybersecurity is to guard the data and integrity of computing tools in an organization's network. The system protects valuable data and information from cyber-attacks and malicious activities. Artificial Intelligence is slowly being incorporated into the business industry and applied in specific cases. Although not all departments are equally advanced, Artificial Intelligence is highly implemented in the information technology and telecommunication sector and least implemented in the automotive industry. According to Kane et al. (2014), beyond 4500 technology decision-makers in various industries, 45 percent of huge organizations and 29 percent of small enterprises have implemented Artificial Intelligence. Thus, artificial intelligence and cybersecurity are vital in securing the neural network.

III. RESEARCH METHODOLOGY

To provide all the information about how the connection of cyber security and artificial intelligence protects neural networks, we used the following database, digital library web science, Scopus, and Google scholar. The paper searched various topics, matched the keyword to provide the best results on this database, and ensured that the report obtained the keywords from the search machine for maximum coverage and provided much accurate information in this research (El Allami et al., 2021). Furthermore, the information gathered was filtered to ensure that the results obtained were from recently published articles. The methodology aims to ensure that the research findings are relevant to modern technology in cyber security and artificial intelligence in securing neural networks (Zafar et al., 2019).

IoT, artificial intelligence, and cyber security are described in depth. Neural networks are the subgroup of machine learning on which they form the primary component of the deep learning algorithms in which their structure and name mimic how the human brain functions. The neural network comprises layers, an output layer, an input layer, and hidden layers (Wang et al., 2018). Neural networks operate when the output layer is activated to transfer the data to the subsequent layer. The neural networks depend primarily on training the data to improve data accuracy over time. These learning techniques are being turned for accuracy to cluster data at high speed and classify them during this learning period. The weight helps neural networks determine the significance of the given variable, in which the more significant variable contributes more to the output than the inputs (O'Shea & Nash, 2015). The inputs are multiplied according to their function and sum the variables. After that, the result is passed via the activation function to determine the quantity of the outputs; if the output exceeds the given threshold, it is transferred to the next layer. Neural networks are defined by how the data is transferred from one layer to another. This research addresses the proper proposal of artificial intelligence methods in neural networks to develop a defensive mechanism to address the challenges and database threats.

IV. IoT-Based Control System And Security Detection

The most notable technology for improving critical infrastructures is IoT-based solutions. If a gadget has an IP address, it can connect to the Internet. Because of the present Internet infrastructure, it is conceivable to state that gadgets linked to the Internet fall under the purview of the IoT idea (Elrawy,et al., 2018). As a result, IoT devices may be vulnerable to practically all hacks that occur in IP-based systems. The Internet's security flaws also wreak havoc on IoT applications. As a result, this new technology has certain cyber-security flaws. Safety of workers and assets, asset theft or pilferage, accidents, associated injuries, and supply chain bottlenecks are frequent difficulties in asset-intensive industries such as manufacturing, utilities, and construction. These difficulties may be solved by enhancing insight into day-to-day operations, replacing old systems with an integrated solution, and automating tedious tasks.

Critical infrastructures in smart heavy industries offer more efficient performance and communication via IoT-based applications. However, this can lead to security flaws and a rise in the number of cyber-attacks on vital infrastructure. The most notable IoT-based cyber-attacks are covered in this report. It is necessary to assess the impact and implications of the situations to comprehend the gravity of the problem (see Fig. 1). In this perspective, the entire set of instances highlights the vulnerabilities in vital infrastructure systems. Insecure configurations in IoT-based control systems frequently cause these flaws (Jin et al., 2020).

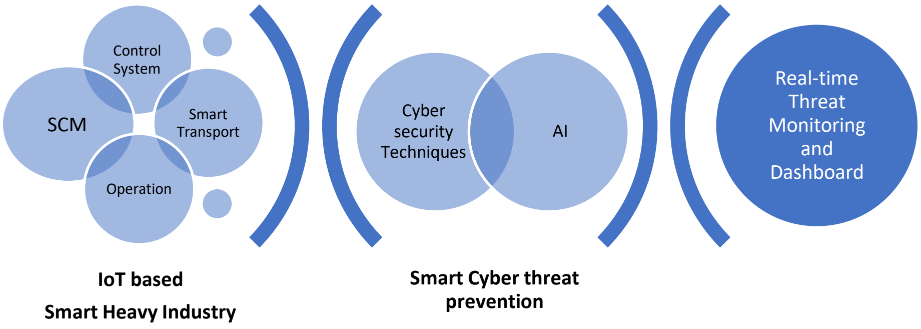
Control System
SCM
Smart Transport
Operation
IoT based
Smart Heavy Industry
Cyber security Techniques
AI
Smart Cyber threat prevention
Real-time Threat Monitoring and Dashboard

Fig 1. Cyberattack monitoring for IoT-enabled innovative industries

DOI: 10.17148/IJARCCE.2022.111008

Computer vision-based solutions with several onboard sensors can aid with lane recognition, traffic signal detection, driver behavior detection, GPS tracking, fuel management, report production, notification alert, and predictive maintenance in today's industries. The motorist obtains assistance in detecting and avoiding accidents while using such solutions. However, these equipment are ideal targets for cybercriminals, who use malware and phishing attacks to control them. It must be prevented using AI-based cyber solutions and continuous monitoring (Sharma et al., 2022). It is also feasible to monitor a heavy machine driver, and automated notifications can be created if the driver is asleep or inactive for an extended period.

V. VULNERABILITIES DETECTION IN NN-BASED DEVICES

Heavy industries have AI-based load balancers to detect the IoT device’s performances and monitor the types of equipment during peak hours. This section explains how the application of artificial intelligence in protecting data leads and load balancing to numerous issues, such as physical challenges (Siddhant et al., 2019). Cyber attackers may use different approaches, for instance, behavior attacks, to extract information. An adversarial artificial intelligence system is where the machine learning algorithms misunderstand the inputs and respond, which may benefit attackers since they can easily access information. Hostile artificial intelligence can occur if the relevant databases do not act upon the appropriate precautions. The system is designed to expose the hackers’ restricting users and appropriately equip the programs using unique emails.

Securing the neural network using cyber security is achieved using an intrusion detection and prevention system. The intrusion detection system can detect all malicious network activities, deter intruders from accessing the information, and signal the users when the system is interfered with. This security method can be identified using genetic attack forms and signatures. This method is mainly used in threats such as data breaches (Gheewala & Patel, 2018). Initially, intrusion detection and prevention methods used machine learning algorithms to secure the data, generating more mistakes, creating massive work for security teams, numerous false positives, and unwarranted fatigue. Neural networks and recurrent neural networks can be applied to develop smaller systems by analyzing the traffic with improved accuracy and minimizing the number of false alerts. This security strategy allows the security team to differentiate the legit and fraudulent network activities.

According to Li et al. (2020), in spam and social engineering detection, a neural network uses the deep learning technique to gather information, which helps detect and arrange spam and other social engineering systems. Natural language processing establishes standard statements that use various numerical models to spot the block spam. With the use of behavior analytics, the organization can track and analyze the behavior and activities of everyone (McCord & Llingworth, 2019). Although it is more challenging since it interacts with security and fails to provide signal behavior, analytics does not provide accurate information since it can pick the expected behavior and detect it as suspicious activity (Ansari et al., 2022).

Organizations undergoing various tests on securing the neural network using artificial intelligence and cyber security realize there are many essential features in the field to be discussed. For instance, the artificial intelligence approach is used primarily in perimeter shooting of the neural network more than cyber security because cyber security cannot address some significant problems. Such major issues include making sound decisions, where the assistant is the major problem cyber security has not solved. Others include comprehensive information, which is much needed to solve the main issues (Kim et al., 2019). Decision-making in artificial intelligence contains many approaches that can solve a complicated situation involving the human brain. Some of these measures are old enough and could have accommodated specific algorithms. However, some methods are no longer considered part of artificial intelligence due to their old nature, which does not apply to the current threats (Siddhant et al.,2019). Artificial intelligence and cyber security approaches have been divided into multiple categories: expert systems, artificial neural, smart agents, computer education, quest constraints resolution, and gathering (Baressi et al., 2020). All these subgroups are designed to protect the neural network in different ways (see Fig 2).

Experts’ system is one of the protection methods. This unique program uses technology to provide the solution raised by a particular technology or the customers from a specific technology in a particular area. The expert system approach is used in decision-making in banks, medical health care, and virtual works (Donkers et al., 2017). The expert system approach can be used to protect data because it provides the solutions to complicated problems starting from the smallest analytical to more advanced systems. The system offers a solution according to its mode of understanding since it contains a deduction engine that analyzes the information fed into the machine system. The vacant understanding, commonly called current plastic understanding, is filled into the system before using it (Shah, 2017). Cyber security and artificial intelligence programs must use the knowledge base software. The improvement has many methods containing artificial

DOI: 10.17148/IJARCCE.2022.111008

intelligence shells that can interpret the information. Experts' system provides stabilization of data as well as interpretation. For security purposes, the system substantially enables the gathering and intrusion of security enterprises to maximize scarce resources. An artificial neural network is the mutual neural network constituent, which can provide fascinating issues by limiting the combination of perceptions (Le et al., 2018). Neural networks include a similar distribution of learning and decision-making ability. he neural networks, operating frequency has a crucial characteristic in which artificial intelligence or cyber security and its application are used to protect the data, such as intrusion detection techniques, software worm identification, forensic science, and zombie identification. When this approach is implemented as quickly as possible, it protects deep learning in computer security (Ansari et al., 2022a). Innovation of neural networks has generated possibilities for various applications, which helps to build many networks and changes in risk.

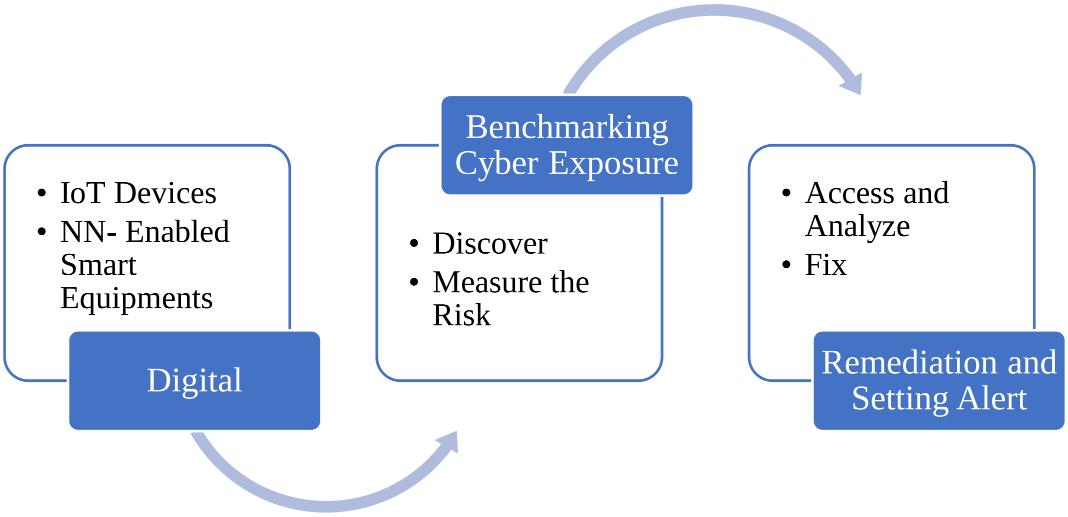
IoT Devices
NN- Enabled Smart Equipments
Digital
Benchmarking Cyber Exposure
Discover
Measure the Risk
Access and Analyze
Fix
Remediation and Setting Alert

Fig 2. Accessing a cyber threat lifecycle in heavy industry

Intelligent agents are software applications whereby the system can prepare, organize, and evaluate the data. This approach uses the networking language (Grosse et al., 2019). An intelligent agent is protecting cooperation from external attacks. The cyber police are responsible for following up with the cyber attackers to prevent cybercrimes. This is possible due to the technology which enables connectivity and mobility that are offed by cyber personnel and must locate the opponents. Naway and Li (2019) state that search involves numerous techniques created to concentrate on a specific problem; the most used search is the dynamic analysis programming to address the security malpractice in the organization. The search uses the minimum cumulative potential loss to establish the knowledge that can be used to protect data. As Chothia and Novakovic (2019) indicated, the information is protected since the authority can monitor any move by the opponent and check any decision made by the responsible management.

VI. DEEP LEARNING AND CYBER DETECTION

Every day, new cyber-attacks develop, and it is extremely difficult to delete them all. However, initial defense tactics are critical in terms of mitigating the impact of current and future attacks. Mitigating cyber-attacks' impacts involves strategies for both intrusion detection and intrusion prevention with real-time processing and monitoring (Dash, 2021). The following are some of the most effective approaches for mitigating the consequences of cyberattacks on IoT-based critical infrastructures (Wang et al., 2022). Deep learning is the technology that is part of the artificial intelligence initiated from the artificial neural network. The deep learning technique can be used intelligently to solve cyber security problems, such as identifying malware in the computer, predicting cyber-attacks, and intrusion detection (Diro & Chilamkurti 2018). Deep learning has many benefits in protecting data since it is more accurate when dealing with the quantity of the database (Nomura et al., 2017). Hybrid security and deep learning approach are used to deal with different ways of cyber security, security threat analysis, and predicting cyber-attack, which contains the following measures.

Multi-layer Perception

Multi-layer perception borrows the idea of the deep neural network, which supervises the learning algorithms. The multi-layer perception consists of input and output (Huang et al.,2017). The input layer is responsible for receiving data, while the output layer is responsible for making decisions. The input and output layers can detect intruders using the implant system, such as the intrusion detection model. This system is most sensitive to attacks, thus giving maximum protection to the system.

Conventional Neural Networks

Chyrun et al. (2019) define a conventional neural network as a unique approach that operates independently depending on the input data, which does not require any manual input feature. The approach is derived from deep learning, which contains numerous layers, and each is stuck on its function. The convolutional neural networks are designed to arrange with the variability of forms, on which it uses the images and video recognition in cyber security. The system can detect only important features automatically without the supervision of a human being; therefore, it is considered one of the most influential models.

Recurrent Neural Network

A recurrent neural network is a system that can cause a sequence of inputs and retain the way it is while continuing with the following sequence of inputs. The recurrent neural network system has a recurrent layer, which helps maintain the same information in an original form, with a special memory to keep information for a long time (Al-Kababji et al., 2019). The recurrent neural network analyses classify processes and make predictions of the data depending on the time series of the data. The system's ability to model the sequence data makes it more advantageous; thus, it can detect security threats, especially behavior patterns.

Self-organizing Map

A self-organizing map is a product of an artificial intelligence network attributed to the unsupervised learning approach. This approach practices a learning algorithm, where the input data are responded to by the competing nodes (Finnerty et al., 2019). The style used by this approach reduces complex problems. A self-organizing map is vital because it is easily understood and interpreted; hence it can develop an effective security model that can be applied anywhere to protect the data.

Auto Encoder

Autoencoder is where codes represent the interpreted data. The autoencoder functions by ignoring some unnecessary signals that the computer can make. The system can bandage the input data, and later the outcome is decoded. The coded data is then reconstructed into various forms the computer can understand. This model is beneficial since it can filter useful information (Wong, 2016). The autoencoder model can be used in the unsupervised model task. Moreover, unlike other models, the model can also use the minimum number of security structures, which makes it more effective as small devices like smartphones can accommodate it.

Restricted Boltzmann Machine

The restricted Boltzmann machine has two nodes, visible nodes and hidden nodes. In this model, every node is linked to each other (Raab & Szekely, 2017). The restricted Boltzmann system is mainly used in practical problems; for instance, an organization may pay someone to hack the organization's data, enabling them to understand how much damage can be caused and the company's vulnerability.

VII. RECOMMENDATIONS

In securing heavy machinery from cyber threats, new techniques and skills must be used to improve security problems using advanced artificial intelligence and cyber security. The research deals more with intrusion detection and malware detection. Autoencoder and recurrent neural network techniques are suitable for detecting information or data threats because of their simplicity and implementation. Adding artificial intelligence to the existing technology can create a broader field to offer more filtered, available, and reliable data. Since technology can provide challenges in protecting information, training staff on handling risk threats should be emphasized.

Securing information should be in multiple forms and legal so that the correct procedure is followed when retrieving the message and tuff penalties on the hackers. The cyber security challenges should be a smarter solution that can counterattack the ideas of hackers. In identifying the over-privileged users, the organization should have full knowledge of who can access the critical information and be ready to conduct a database review to ensure that the information is intact and the administration has the privilege to perform their work. Database monitoring should be undertaken to establish the best implementation for securing data. Data monitoring enables the security team intelligence to conduct prompt action if a violation occurs and detect the threats.

DOI: 10.17148/IJARCCE.2022.111008

VIII. CONCLUSION

Artificial intelligence and cyber security strategies cannot be overlooked due to rising cyber threats, and malicious intelligence is gaining momentum. Therefore, every heavy industry must protect its data using smart approaches and minimum resources. Artificial intelligence and cyber security approaches must be implemented to ensure the database is secure and information is controlled. Neural network threats can only be overcome if cyber securities and artificial intelligence are deployed. Information technology should lead to the improvement of civilization; by accomplishing tasks faster, with accuracy, and with fewer errors. Artificial intelligence approaches such as intrusion detection and deep learning should be strengthened using modern technology. The neural network system combines software, trained personnel, and hardware to facilitate control, decision-making, and planning in an organization. Securing an IoT device involves controlling and keeping the information for the organization’s growth.

REFERENCES

[1]. Al-Kababji, A., Shidqi, L., Boukhennoufa, I., Amira, A., Bensaali, F., Gastli, M.S., Jarouf, A., Aboueata, W. and Abdalla, A., 2019, August. IoT-based fall and ECG monitoring system: wireless communication system based firebase realtime database. In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 1480-1485). IEEE.

[2]. Ansari, M.F., Sharma, P.K. and Dash, B., 2022. Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. Prevention.

[3]. Ansari, M.F., Dash, B. and Sharma, P., 2022a. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. https://doi.org/10.17148/ijarcce.2022.11912

[4]. Baressi Šegota, S., Lorencin, I., Musulin, J., Štifanić, D. and Carr, Z., 2020. Frigate speed estimation using CODLAG propulsion system parameters and multilayer perceptron. NAŠE MORE: znanstveni časopis za more i pomorstvo, 67(2), pp.117-125.

[5]. Chothia, T. and Novakovic, C., 2015. An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

[6]. Chyrun, L., Gozhyj, A., Yevseyeva, I., Dosyn, D., Tyhonov, V. and Zakharchuk, M., 2019. Web Content Monitoring System Development. In COLINS (pp. 126-142).

[7]. Dash, B., 2021. A hybrid solution for extracting information from unstructured data using optical character recognition (OCR) with natural language processing (NLP).

[8]. Dash, B. and Ansari, M.F., 2022. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

[9]. Diro, A.A. and Chilamkurti, N., 2018. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, pp.761-768.

[10]. Donkers, T., Loepp, B. and Ziegler, J., 2017, August. Sequential user-based recurrent neural network recommendations. In Proceedings of the eleventh ACM conference on recommender systems (pp. 152-160).

[11]. Elrawy, M.F., Awad, A.I. and Hamed, H.F., 2018. Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), pp.1-20.

[12]. El-Allami, R., Marchisio, A., Shafique, M. and Alouani, I., 2021, February. Securing deep spiking neural networks against adversarial attacks through inherent structural parameters. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 774-779). IEEE.

[13]. Finnerty, K., Fullick, S., Motha, H., Shah, J.N., Button, M. and Wang, V., 2019. Cyber security breaches survey 2019.

[14]. Gheewala, S. and Patel, R., 2018, February. Machine learning-based Twitter Spam account detection: a review. In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC) (pp. 79-84). IEEE.

[15]. Grosse, K., Paper not, N., Manoharan, P., Backes, M. and McDaniel, P., 2017, September. Adversarial examples for malware detection. In European symposium on research in computer security (pp. 62-79). Springer, Cham.

[16]. Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., Liu, T., Wang, X., Wang, G., Cai, J. and Chen, T., 2018. Recent advances in convolutional neural networks. Pattern Recognition, 77, pp.354-377.

[17]. Huang, H.B., Li, R.X., Yang, M.L., Lim, T.C. and Ding, W.P., 2017. Evaluation of vehicle interior sound quality using a continuous restricted Boltzmann machine-based DBN. Mechanical Systems and Signal Processing, 84, pp.245-267.

[18]. Jin, R., Zhang, H., Liu, D. and Yan, X., 2020. IoT-based detecting, locating and alarming of unauthorized intrusion on construction sites. Automation in Construction, 118, p.103278.

DOI: 10.17148/IJARCCE.2022.111008

[19]. Kim, U.H., Park, J.M., Song, T.J. and Kim, J.H., 2019. 3-d scene graph: A sparse and semantic representation of physical environments for intelligent agents. IEEE transactions on cybernetics, 50(12), pp.4921-4933.

[20]. Li, Z., Jiao, Z. and He, A., 2020. Knowledge-based artificial neural network for power transformer protection. IET Generation, Transmission & Distribution, 14(24), pp.5782-5791.

[21]. McCord-Nelson, M. and Illingworth, W.T., 2019. A practical guide to neural nets. Addison-Wesley Longman Publishing Co., Inc.

[22]. Naway, A. and Li, Y., 2019. Using deep neural network for Android malware detection. arXiv preprint arXiv:1904.00736.

[23]. Nomura, Y., Darmawan, A.S., Yamaji, Y. and Imada, M., 2017. Restricted Boltzmann machine learning for solving strongly correlated quantum systems. Physical Review B, 96(20), p.205152.

[24]. O'Shea, K. and Nash, R., 2015. An introduction to convolutional neural networks. arXiv preprint arXiv:1511.08458.

[25]. Raab, C. and Szekely, I., 2017. Data protection authorities and information technology. Computer Law & Security Review, 33(4), pp.421-433.

[26]. Shah, N., 2017. Securing Database Users from the Threat of SQL Injection Attacks.

[27]. Sharma, P., Dash, B. and Ansari, M.F., 2022. Anti-Phishing Techniques–A Review of Cyber Defense Mechanisms.

[28]. Kane, G.C.J., Palmer, D., Phillips, A.N., Kiron, D. and Buckley, N., 2014. Moving beyond marketing: Generating social business value across the enterprise. MIT Sloan Management Review, 56(1), p.1

[29]. Hatfield, J.M., 2018. Social engineering in cybersecurity: The evolution of a concept. Computers & Security, 73, pp.102-113.

[30]. Siddhant, A., Goyal, A. and Metallinou, A., 2019, July. Unsupervised transfer learning for spoken language understanding in intelligent agents. In Proceedings of the AAAI conference on artificial intelligence (Vol. 33, No. 01, pp. 4959-4966).

[31]. Wang, S., Li, Y., Zhang, J., Meng, Q., Meng, L. and Gao, F., 2020, November. PM2. 5-GNN: A Domain Knowledge Enhanced Graph Neural Network For PM2. 5 Forecasting. In Proceedings of the 28th International Conference on Advances in Geographic Information Systems (pp. 163-166).

[32]. Wong, A., 2016. Cybersecurity: Threats, Challenges, Opportunities. Retrieved, 11(15), p.2017.

[33]. Zafar, S., Nazir, M., Sabah, A. and Jurcut, A.D., 2021. Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based parameter profiling. Computers in Biology and Medicine, 136, p.104707.

[34]. Potluri, S., Ahmed, S. and Diedrich, C., 2020. Securing Industrial Control Systems from False Data Injection Attacks with Convolutional Neural Networks. In Development and Analysis of Deep Learning Architectures (pp. 197-222). Springer, Cham.

BIOGRAPHY

Smrutirekha is an engineering student in her last year at the Government College of Engineering in Keonjhar, Odisha, India. Her primary research interests are in power electronics and control systems with an emphasis on AI and IoT. She is passionate about technical transformation and always enjoys reading scientific studies and periodicals on emerging technologies.