EFFECTIVE MALWARE DETECTION APPROACH BASED ON DEEP LEARNING IN CYBER-PHYSICAL SYSTEMS

Srinivas Aditya Vaddadi[1], Pandu Ranga Rao Arnepalli[2],
RamyaThatikonda[3], Adithya Padthe[4]

Doctor of Philosophy, Information Technology, University of the Cumberlands, USA

ABSTRACT

Cyber-physical Systems based on advanced networks interact with other networks through wireless communication to enhance interoperability, dynamic mobility, and data supportability. The vast data is managed through a cloud platform, vulnerable to cyber-attacks. It will threaten the customers in terms of privacy and security as third-party users should authenticate the network. If it fails, it will create extensive damage and threat to the established network and makes the hacker malfunction the network services efficiently. This paper proposes a DL-based CPS approach to identify and mitigate the malware cyber-physical system attack of Denial of Service (DoS) and Distributed Denial of Service (DDoS) as it ensures adequate decision support. At the same time, the trusted user nodes are connected to the network. It helps to improve the privacy and authentication of the network by improving the data accuracy and Quality of Service (QoS) in the network. Here the analysis is determined on the proposed system to improve the network reliability and security compared to some of the existing SVM-based and Apriori-based detection approaches.

KEYWORDS

Cyber-Physical System, Security, Deep learning, DoS, DDoS, Authentication.

1. INTRODUCTION

Network-related activities are rising rapidly every day, and confidential information is expanding significantly. In this situation, the network faces issues related to security as intruders, i.e., Unauthorized users, contain those activities that are malicious and have any unwanted activities. Mainly, the intruder intends to attempt the confidential data [1]. Based on the various security-based network methods, they are overcoming the attacks and illegal activities on the physical systems through cyber-attacks. It still exists on it even though the methods are applied to it. So, an effective intrusion system should be needed to prevent those attacks based on the system related to the network intrusion approach. Several intrusion systems exist in the current scenario as there are broadly classified as Denial of Service (DoS) [2], Cross-Site Scripting (CSS) [3],etc., and are used to overcome the attacks that still exist.

In this case, the network will have different services so that cyber-physical systems will associate with cyber systems with some physical processors based on many loops. Many IoT-based sensors are added such that actuators and other elements are added and integrated and form a network structure [4]. The above will helps to create a network so that they can communicate through TCP/IP-like network-oriented connections and many protocols related to wireless networks. Then the system about cyber-physical will have many intrusions that are prone to the network, which is simple in structure. The cyber-based systems will make the system safe and secure; even system

DOI: 10.5121/ijcsit.2022.14601

failure will happen and trigger based on the attacks. The intruder will cause more damage to the system even based on the system being controlled, and people will depend on those systems. Thus, the above scenario can avoid attacks based on cyber-physical systems with effective network intrusion systems [5]. Then the cyber-physical systems will be triggered to generate the resource and process the physical systems. This makes it be controlled physically through the process of network computation and network communication through the connection of network devices.

These network devices will enable the access of the resource remotely and control the network devices and systems of cyber-physical and various network machines, making them more critical and essential for multiple industrial scenarios [6]. When the users are more dependent on the cyber system, the methods get executed on the implementation of different security threats, and it may result in severe damage to the objects of the physical nature system. Also, it will directly reflect on the users who now depend on those cyber systems. Finally, the effective network intrusion detection system will execute activities to avoid those that damage the system based on network attacks.

The Internet of Things (IoT) is considered an important medium to communicate with the world through IoT devices and make everything possible. Through IoT devices, we can achieve our daily activities in a facilitated way. Some IoT devices include smartphones, intelligent E-bikes, autonomous cars, smart temperature sensors, etc., which can be applied in various fields. As a result of these tremendous results, data generation will be in large volume from IoT devices and their supporting platforms. These data should be transmitted and stored through back-end storage centerssuch as Cloud infrastructure. Some unique computing capabilities are needed to compute the large volume of data other than regular traditional extensive data analysis. IoT devices generate continuous streaming data, which is in raw format. These data directly cannot be handled for storage and another process [7]. These data should be processed and cleaned to extract the meaning of complete information and knowledge from the raw data. The next step is to handle the heterogeneity of data from different IoT devices, dependent on the application domain of e-health, intelligent vehicles, smart electricity grids, innovative home management, etc. IoT's impact on business fields will be more in the coming years, as per the survey from McKinsey's report. The economic impact of IoT-based services will boom the growth of many sectors to a new level. The annual economic impact of IoT in 2025 will be between $2.7 to $6.2 trillion. The result of IoT in various sectors in 2025 [8] is in Figure 1.

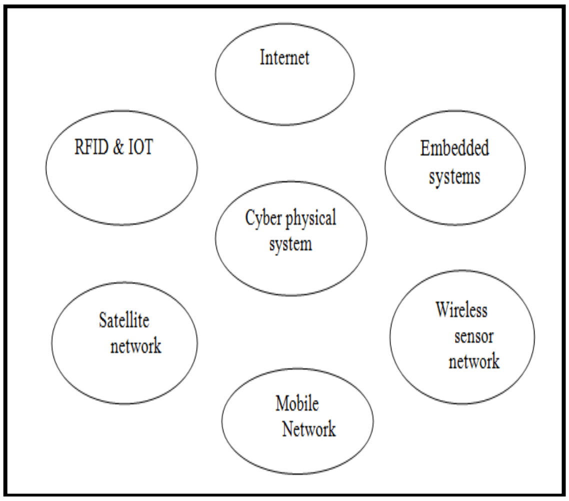

Figure 1. Components of Cyber-Physical System.

The research objective is mentioned below,

- The modified deep learning approach based on Cyber-Physical Systems (CPS) is proposed to effectively process those IoT-based data with enhanced data security.
- Based on the deep learning model, Modified DL-basedAuto-Encode to perform the data processing effectively.
- The modified data access algorithm helps to process the raw data generated from IoT from time to time, and it helps to convert the data to knowledge data.
- Then the data are secured based on policy access control against attacks like DoS and DDoS.
- The performance analysis approach helps to provide an effective classification of data and reliable data to be maintained. The security of IoT data is to be verified against DoS and DDoS attacks on cyber-physical systems in real-time applications.

The paper is organized as follows; the existing works are discussed in section 2. Then the research methodology is discussed in section 3. The performance analysis with accuracy and execution time is analyzed in section 4. Finally, the conclusion is discussed in section 5.

2. LITERATURE SURVEY

In the literature survey, intrusion-based network systems will play a vital role in the research area. Various machine learning approaches still exist and are proposed as the related study in the current scenario. Then multiple datasets are used as generated ones that are analyzed and refined through various learning models. Initially, these machine learning models are being used on the intrusion network systems that are added and integrated to make salient information such as selection of features, paradigm integration, and various deep learning models [9]. The critical activities in cyber-physical systems are intrusion detection systems that can keep track of the essential feature with adequate quality to identify the data and remove unwanted or irrelevant information features [10].

It makes to reduce the feature dimension based on the datasets that are used. Then [11-13] propose the hybrid method, which integrates both a Support Vector Machine (SVM) and a Genetic Algorithm (GA).It analyses and extracts the datasets through a learning algorithm, making the genetic algorithm more efficient than the support vector machine. Then the learning algorithm will make associated with feature subset selection. [14]Proposed a malware detection model associated with cloud computing based on packet networking. Identifying packets, considered the input, uses data mining to reduce the packet knowledge, which helps to validate whether malware is detected. Data mining will analyze data extraction, but the learning algorithm will learn the input dataset. So, SMMDS based malware detection model will follow the machine learning technique in table 1.

Table 1. Various ML / DL Methods based on Data Processing

ML methods / DL Methods	**Data processing Type**	**Outcome**
K-nearest neighbor (KNN)	Classification	Tree-based search [15]
Support Vector Machine(SVM)	Classification	Detection of microcalcification clusters in digital mammograms [16]
Multiple Linear Regression	Regression	Estimation of market values of the football players in the forward positions [17]
Random Forests	Classification and Regression	analysis of significant genome-wide association (GWA) datasets [18]
Daily Consumption Estimation Network and Intraday Load Forecasting Network	Edge devices, Control Center in Cloud	Smart meters (for different electronic gadgets) [19]

The framework is proposed to extract the feature during the installation of mobile applications and execute them. Then, the machine learning technique[20] components are trained using machine learning algorithms to perform data classification, which helps identify the malware. Here in this approach, substantial system resources and data loading time are limited. The proposal works to construct a detection-based malware detection model, and an anomaly occurs in mobile applications [21]. To operate feature information, some machine learning algorithms such as naïve Bayes and logistics calculate the accuracy rate among the data [22]. As in this approach, specific parameters are not considered, as mentioned, CPU utilization, data memory, battery, and training data as the limitations in Table 2.

Table 2. Existing Work Comparison based on deep learning based Error Detection

S.No.	**Title of the paper**	**Techniques used**	**Merits**	**Gap Identified**
1	Deep Learning: Edge-Cloud Data Analytics for IoT[23]	Auto Encoders in the Edge-machine learning in the Cloud IoT data analytics	Dimensionality reduction	It needs further investigation to improve services; handling high-dimensional data is not given.
2	Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing [24]	They are deep Learning for IoT in the EDGE computing environment using multiple CNN and process scheduling.	Increased data processing while performing in an EDGE computing environment.	There is a need for practical implementation.
3	A Comparative Study of ClassificationTechniques for Managing IoT Devices of Common Specifications [25]	WEKA data mining tool, KNN, Naïve Bayes, SVM, Random Forest	Worked on different classification algorithms and proposed the best matching algorithm	I still have to work with different classification algorithms with varying data sets to implement them practically.
4	Deep Learning and Big Data Technologies for IoT Security [26]	TensorFlow, Pytorch, Anomaly detection, Malware detection	Different Deep Learning architectures and Big Data technologies were discussed	Execution time extends with implementing big data and DL technologies in IoT data.
5	IoT Data Processing: The Different Arch types and Their Security and Privacy Assessment [27]	Mobile-Edge Computing, Cloudlets, and discussions on different Security policies	Security threats at each level of the data processing layer are discussed.	Needs further discussion on Security policies and risk calculations in the EDGE or Cloud environment.

3. Research Methodology

IoT-connected devices will touch 25 billion by 2022, according to research. IoT devices generate huge volumes that should be pre-processed to avoid noisy, unlabeled, and missing data. Data should be processed to extract knowledge from the information data.By implementing an appropriate DL model, we can achieve the desired output[28].In IoT search technology, intelligent devices access personal information like health, age, etc., which threatens privacy data. An effective access control mechanism is needed to secure the data classified from IoT devices. Some of the existing algorithms for Data security are categorized based on centralized, distributed, and hybrid. Deep learning represents a new field in machine learning research that places the network in the form of large numbers of examples at a given level of accuracy.

In recent years, profound learning algorithms have been improved to a high standard and proven to be extraordinary precision. Because of its higher accuracy is an obvious option in various industries, including automatic driving, aerospace, defense systems, defense science, and the advertising industry [29]. The main benefit of deep learning is that the size of the label data increases and will continue to improve its accuracy. Many new libraries are being built and available as a relatively recent phenomenon. TensorFlow, a development team of Google's Google Brain team in the Research Center for Machine Intelligence, was initially created by scientists and engineers.

Deep learning and deep neural networks are particularly relevant in machine learning techniques to take into account (DNN)[30]. These revolutionized artificial intelligence with the advent of high-computing GPUs in several fields of engineering and IT. While IDS' DNN technology is still in its early stages, several examples of its application in cyber security do occur. It used the KDDCup '99 dataset in its study for Long Short Term memory (LSTM). The LSTM-RNN achieved a precision of 96.93% and 98.88% memory.

Abolhasanzadeh used an automatic deep encoder as a data attack detector. The test performed on the NSL-KDD test set was used to detect intrusions for dimensional bottleneck reduction. It was concluded that intrusion detection in the real world was accomplished with the accuracy promised as it considers using a limited Boltzmann computer (RBM). The network can be used for the identification of anomalies by learning from a real-world dataset for 24 hours. Alom provided several experiments to the Deep Belief Network (DBN) for performing intrusion detection. To distinguish unforeseen attacks, the authors trained the DBN on NSL-KDD. The invention of GPU card hardware and computing capabilities makes DNN processes an excellent alternative to conventional approaches and a panacea for overcoming the problems facing CIP institutions.

3.1. Deep Learning Methods On Cyber Attack Detection

A network attack detection approach is proposed based on a sparse self-encoder and self-trained DL. For unattended learning tasks, the large self-encoder is first used. The learning functions are subsequently fed into the deep regression pattern in attacks and standard classification of the data. This is resolved by using the Deep RNN (RNN-Aes) process. API requests allow the auto encoder to learn the representations of malware—Application Program Interface. APIMDS is used in testing. The LSTM-based decoder method is proposed.

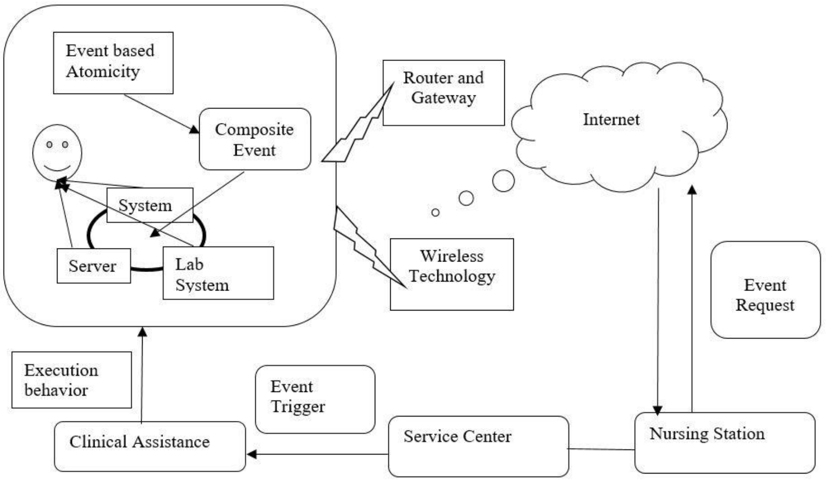

Figure 2. DL-based CPS for Hospital Monitoring System.

The CAPTCHA images are not publicly identified. The CAPTCHA generation software is used to create experimental data in this area. The malware detection model based on DL comprises Stacked Auto Encoders (SAEs) and is known as DL4MD. The method has two key components: extraction of the function and classification of DL. In two steps, the model detects malware: unsupervised pre-train back propagation monitored. This network's data was extracted using Windows API calls from Portable Executable (PE) files. The method can be validated using data from the Comodo Cloud Security Center, including samples of files, malware, benign files, and unfamiliar files.

Deep learning and big data technologies have been discussed in IoT data security and processing data [14].Some existing Deep learning architectures include Autoencoder, recurrent neural network, and DBN. Etc. Those DL-based architectures are implemented.

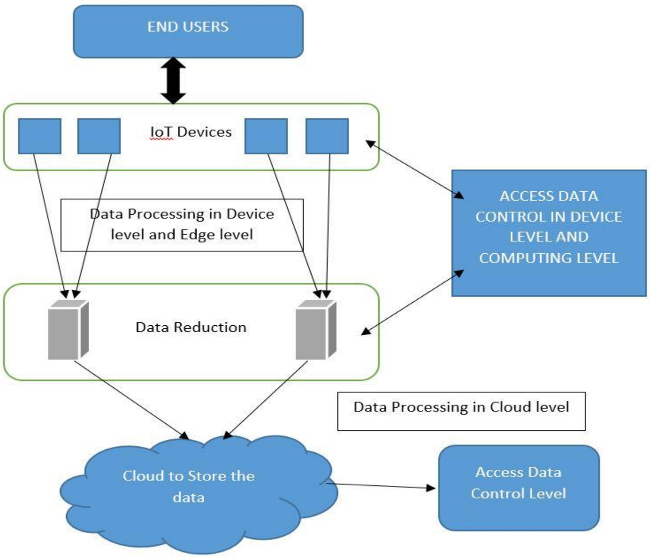
END USERS
IoT Devices
Data Processing in Device level and Edge level
ACCESS DATA CONTROL IN DEVICE LEVEL AND COMPUTING LEVEL
Data Reduction
Data Processing in Cloud level
Cloud to Store the data
Access Data Control Level

Figure. 3. Data Processing with Cloud Security with data reduction

Figure 3 gets processing the data, which is being transferred/exchanged in the framework of DL-based CPS for Hospital Monitoring System in Figure 2 as some confidential data are communicated between the patients / Users, hospital doctors, nurses, etc.

They are using TensorFlow, Caffe, PyTorch., etc. Existing security applications of IoT include Anomaly detection, Host Intrusion Detection System, and Malware Detection in Figures 2 and 3.There are specific limitations to the existing work mentioned below, Limited Datasets, Detection rate efficiency, and Effective computation rate.

Algorithm 1: Modified DL-based Auto-Encode for Reducing the Data

```
Input: Data' d'
Output: Original Data Extraction
Initialize the data 'd'
Data are processed through the hidden layer
Auto encoder to learn to data representation 'R(d).'
Auto-Coder:
R(d) → Compress the data
Compress the data based on Random and Random Shuffle Functions;
```

```
Bit Interleaving Process
Compress data → Abstract Data Representation
Reconstructing the data (Decoder)
Compress the data based on Random and Random Shuffle Functions;
Reverse Bit Interleaving Process
Abstract Data Representation→ Original Data
```

In algorithm 1, modified deep learning makes some automated processes as it helps to reduce the data processing based on the data input. Those data are processed using a hidden layer as it makes data representation using an auto-encoder. Initially, the data gets compressed in the form of a polynomial equation. The data are compressed based on random and random shuffle functions. Then the data are performed with some interleaving process, and the compressed data is into abstract data representation. Then, the decoding process is recompressed based on random and random shuffle functions, and a reverse bit interleaving process is performed to restore the original data. In algorithm 2, service security is initiated based on the encoder and decoder module.

Algorithm 2: Encoder and Decoder Service Initiation

```
Input: Datasets
Output: Base Decoder
// Encoder
Encoder (Module)
Definition Init
        Super (Encoder). Initiation
Definition Forward
        Raise Error
//Decoder
Decoder (Module)
Definition Init
        Super (Decoder). Initiation
Definition Initiation State
        Raise Error
Definition Forward
        Raise Error
```

b. Security Verification Algorithm

1. The user requested access to the gateway
2. The gateway gets authorization decisions from Packet Data Protocol (PDP)
3. PDP will evaluate the local policies in it
4. PDP sends the decision authority
5. Finally, the gateway will send the user the accepted (or) rejected access.

// Distributed Approach

6. Initialize the user, gateway, and device-associated packet data protocol.
7. The above same process gets repeated for the distributed approach.

In this study, the larger datasets can be applied to the performance analysis, and a few more attributes can be considered. As the limitations of this study, security verification and validation can be performed on the security tool concerning DoS and DDoS.

4. Performance Analysis

In this performance analysis, 30,000 datasets are considered based on SCADA as it contains Source packets, total packets, total bytes, source ports, destination packets, and source bytes as it helps to perform data pre-processing. To calculate the data classification activity by varying the input based on sizes. Based on table 3, calculate the recall based on feature subset extraction based on various intrusions like DDoS, SQL injection, etc. the recall with DDoS and SQL injection is performed in the proposed approach based on the number of Epochs as it gets varied from 10 to 50. Table 3 inferred that the Recall value gradually increases as the number of epochs increases.

Table 3. Recall based Various Epochs

Epochs	Recall DDoS	Recall SQL Injection
10	0.98	0.99
20	0.87	0.92
30	0.84	0.89
40	0.82	0.85
50	0.78	0.81

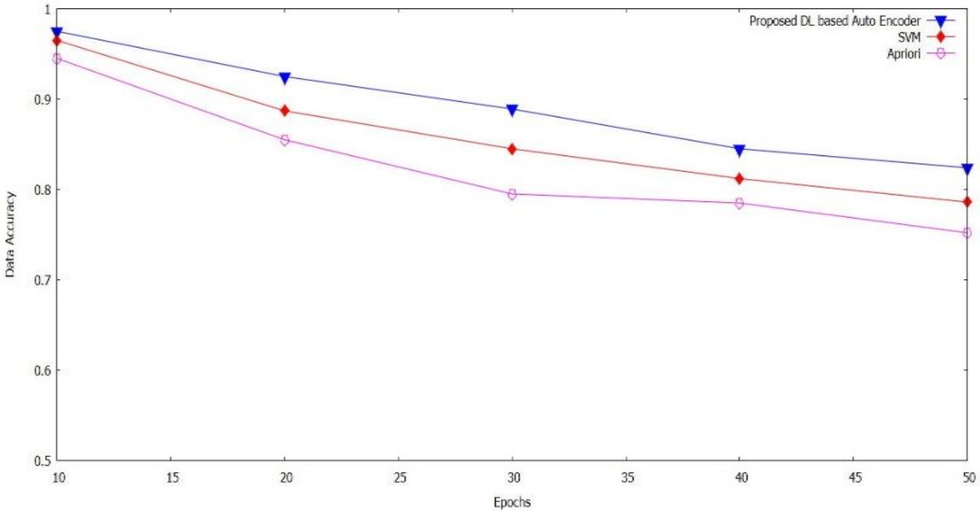

Figure 4. Data Accuracy based on the number of Epochs

Figure 4 shows data accuracy for the proposed system concerning test and train data by varying the epoch from 10 to 50. The data accuracy increases and performs effectively for the proposed DL compared to the existing SVM and Apriori algorithms. Based on the number of epochs, the average data accuracy gradually increases for the proposed one.

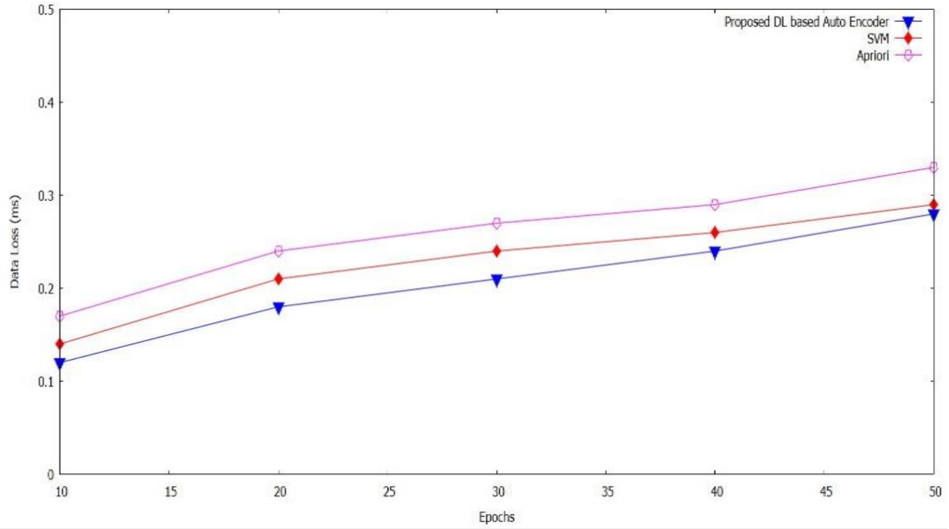

Figure 5. Data Loss based on the number of Epochs

Figure 5 shows data loss for the proposed test and train data system by changing the epoch from 10 to 50. Failure in the data gets reduced for the proposed DL compared to the other existing algorithms, such as SVM and Apriori. The Average data loss gets lower even if the number of epochs increases for the proposed DL-based approach.

5. CONCLUSION

To develop a framework for Data processing in each level of IoT devices and to provide data security. Data processing can be done at Fog/ Edge and Cloud levels. Access Control mechanisms will be applied at each level to handle the data securely. Data processing and access control will be combined as a single unit in this framework to provide quality classification in data and reliable, efficient, and scalable IoT security solutions. The feature selection approach helps to minimize the featured datasets and perform better. Then featured set can identify the malware with data misclassification-based errors with better accuracy. Then apply a machine learning algorithm to provide better detection and computation. In future work, advanced deep learning can be used in managing significant data processing and in real-time applications.

REFERENCES

[1] Mitchell, R.,&Chen, I., (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 6(4), 1-26. https://doi.org/10.1145/2542049.

[2] Zhao, L.,& Long, W., (2020). Co-Design of Dual Security Control and Communication for Nonlinear CPS UnderDoS Attack. IEEE Access, 8, 19271 – 19285.DOI: 10.1109/ACCESS.2020.2966281.

[3] Lin, H., Hu, J., Ma, J., Xu, L., &Yu, Z., (2017). A Secure Collaborative Spectrum Sensing Strategy in Cyber-Physical Systems. IEEE Access. 5, 27679 – 27690.DOI: 10.1109/ACCESS.2017.2767701.

[4] Isakovic, H.,Ratasich, D., Hirsch, C.,Platzer, M., Wally, B., Rausch, T.,Nickovic, D.,Krenn, W., Kappel, G.,Dustdar, S.,&Grosu, R., (2018). CPS/IoT Ecosystem: A Platform for Research and Education. In Proceedings of International Workshop on Design, Modeling, and Evaluation of Cyber-Physical Systems Workshop on Embedded Systems and Cyber-Physical Systems Education CyPhy (pp. 206-213). DOI: 20.500.12708/57632.

[5] Wang, L., Qu, Z., Li, Y., Hu, K., Sun, J.,Xue, K., &Cu, M., (2020). Method for Extracting Patterns of Coordinated Network Attacks on Electric Power CPS Based on Temporal–Topological Correlation. IEEE Access, 8, 57260 – 57272. DOI: 10.1109/ACCESS.2020.2982057.

[6] Pan, F., Pang,Z., Wen, H.,Luvisotto, M., Xiao, M., Liao, R., & Chen. J., (2019). Threshold-Free Physical Layer Authentication Based on Machine Learning for Industrial Wireless CPS. IEEE Transactions on Industrial Informatics, 15(12), 6481 – 6491. DOI: 10.1109/TII.2019.2925418.

[7] Cheng, B., Zhang, J.,Hancke, G. P., Karnouskos, S.,& Colombo, A. W., (2018). Industrial Cyberphysical Systems: Realizing Cloud-Based Big Data Infrastructures. IEEE Industrial Electronics Magazine, 12(1), 25 – 35. DOI: 10.1109/MIE.2017.2788850.

[8] Li, L., (2018). China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0. Technological Forecasting and Social Change, Elsevier, 135, 66 – 74. https://doi.org/10.1016/j.techfore.2017.05.028.

[9] Bagula, A., Ajayi, O.,&Maluleke, H., (2021). Cyber-Physical Systems Dependability Using CPS-IoT Monitoring. Sensors, 21(8). DOI: 10.3390/s21082761.

[10] Oyekanlu, E., (2018). Fault-Tolerant Real-Time Collaborative Network Edge Analytics for Industrial IoT and Cyber-Physical Systems with Communication Network Diversity. In Proceedings of IEEE 4th International Conference on Collaboration and Internet Computing (CIC).DOI: 10.1109/CIC.2018.00052.

[11] Gressl, L.,Krisper, M., Steger, C.,&Neffe, U., (2020). Towards an Automated Exploration of Secure IoT/CPS Design-Variants. In Proceedings of International Conference on Computer Safety, Reliability, and Security SAFECOMP 2020: Computer Safety, Reliability, and Security, 372 – 386. DOI:10.1007/978-3-030-54549-9_25.

[12] Tu, M., Lim,M. K. &Yang, M., (2018). IoT-based production logistics and supply chain system – Part 2: IoT-based cyber-physical system: a framework and evaluation. Industrial Management & Data Systems, Industrial Management & Data Systems, 118(1), 96-125. https://doi.org/10.1108/IMDS-11-2016-0504

[13] Aslahi-Shahri,B.M.,(2016). A hybrid method consisting of GA and SVM for the intrusion detection system. Neural ComputAppl, 27, 1669-1676. https://doi.org/10.1007/s00521-015-1964-2.

[14] Sun, S., Ye, Z., Yan, L., Su, J., &Wang, R., (2018). Wrapper feature selection based on lightning attachment procedure optimization and support vector machine for intrusion detection. In Proceedings of the IEEE 4th international symposium on wireless systems within the international conferences on intelligent data acquisition and advanced computing systems, IDAACS-SWS (pp. 41–6). DOI: 10.1109/IDAACS-SWS.2018.8525742.

[15] Raza, S., Wang, S., Ahmed, M., &Rizwan Anwar, M., (2019). A Survey on Vehicular Edge Computing: Architecture, Applications, Technical Issues, and Future Directions, Hindawi Wireless Communications and Mobile Computing, 3159762. https://doi.org/10.1155/2019/3159762.

[16] El-Naqa, I., Yang, Y.,Wernick, M.N.,Galatsanos, N.P., & Nishikawa, R.M., (2002). A Support Vector Machine Approach for Detection of Micro calcifications. IEEE Transactions on Medical Imaging. 21(12), 1552 – 1563.DOI: 10.1109/TMI.2002.806569.

[17] Li, S., (2018). A Multiple Linear Regression Approach For Estimating the Market Value of Football Players in Forwarding Position. The Frontiers of Society, Science and Technology. 2(15). 132-143. DOI: 10.25236/FSST.2020.021516.

[18] Goldstein,B. A., Hubbard, A.N., Cutler, A., &Barcellos, L.F.,(2010). An Application of Random Forests to a genome-wide association dataset: Methodological considerations & new findings. BMC Genetics.DOI: 10.1186/1471-2156-11-49.

[19] Li, L.,Ota, K., &Dong, M., (2017). When Weather Matters: IoT-Based Electrical Load Forecasting for Smart Grid. IEEE Communications Magazine. 55(10). 46-51. DOI: 10.1109/MCOM.2017.1700168.

[20] Yi, S., Hao, Z., Qin, Z., &Li, Q., (2015). Fog computing: Platform and applications. In Proceedings 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb), (pp. 73–78).DOI: 10.1109/HotWeb.2015.22.

[21] Jagadish, H.V.,Ooi, B.C., Tan, K.-L., Yu, C., &Zhang, R., (2005). I distance an adaptive bþ-tree based indexing method for nearest neighbour, ACM Trans. Database Syst. (TODS), 30 (2). 364–397. https://doi.org/10.1145/1071610.1071612.

[22] Mohammadi,M., Al-Fuqaha, A.,Sorour,S., &Guizani, M., (2018). Deep Learning for IoT Big Data and Streaming Analytics- A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960. DOI: 10.1109/COMST.2018.2844341.

[23] Ananda M. Ghosh&Grolinger, K., (2019). Deep Learning: Edge-Cloud Data Analytics for IoT, IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). DOI: 10.1109/CCECE.2019.8861806.

[24] Li, L.,Ota, K., &Dong, M., (2018). Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing, IEEE Network, 32(1): 96-101.DOI: 10.1109/MNET.2018.1700202.

[25] Mavrogiorgou, A.,Kiourtis, A., &Kyriazis, D., (2017). A Comparative Study of Classification Techniques for Managing IoT Devices of Common Specifications, In Proceedings of International Conference on the Economics of Grids, Clouds, Systems, and Services, (pp. 67-77). https://doi.org/10.1007/978-3-319-68066-8_6.

[26] Amanullah, M.A., Habeeb, R.A.A.,Nasaruddin, F.H.,Gani, F., Ahmed, E., Nainar, A.S.M., Akim, N.M., & Imran, M., (2020). Deep learning and big data technologies for IoT security, Computer Communications, 151, 495-517. https://doi.org/10.1016/j.comcom.2020.01.016.

[27] Pramanik, P.K.D., &Choudhury, P., (2018). IoT Data Processing: The Different Archetypes and Their Security and Privacy Assessment, Internet of Things Security.DOI:10.1201/9781003338642-3.

[28] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728

[29] Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network., 61–72.https://doi.org/10.47893/ijssan.2022.1221

[30] Ansari, M. F., & Dash, B. (2022). Self-service analytics for data-driven decision making during COVID-19 pandemic: An organization's best defense. Academia Letters. https://doi.org/10.20935/al4978

AUTHORS

Srinivas Aditya Vaddadi, Senior DevSecOps architect with 8 plus years of experience in the IT industry. Currently pursuing PhD in Information Technology at University of the Cumberlands with a topic of exploring the effectiveness of cybersecurity training in the healthcare industry.

PanduRanga Rao Arnepalli, working as Software Development Engineer in Test(SDET) with 5 plus years of professional experience. Currently pursuing PhD in Information Technology at University of the Cumberlands with topic of exploring the 'Factors Influencing Trust in Online Retailing.

Ramya Thatikonda, Ph.D. graduate in Information Technology at University of the Cumberlands and currently working as a Technology Specialist for Wal-Mart in Arkansas.

Adithya Padthe, I am an Information Technology research student. I have 7+ years of IT experience. I work on Einstein Analytics.