Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

IoT-ENABLED CYBER-PHYSICAL SYSTEMS: TOWARDS DETECTION AND ATTRIBUTION OF CYBER-ATTACKS

Mrs.PVN RAJESWARI Associate Professor in Department of CSE, PBR Visvodaya Institute of Technology & Science, Kavali.

V VARSHITHA, S MINALI, R LAKSHMI LIKHITHA, M VINEELA.B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute of Technology & Science, Kavali.

ABSTRACT: Cyber-physical systems (CPS) that are Internet of Things (IoT) enabled can be difficult to secure because security measures designed for general information/operational technology (IT/OT) systems may not work as well in a CPS environment. Thus, a two-level ensemble attack detection and attribution framework for CPS—and more specifically, an industrial control system (ICS)—is presented in this article. For detecting attacks in unbalanced ICS environments, a decision tree combined with a novel ensemble deep representation-learning model is developed at the first level. An ensemble deep neural network is created to facilitate attack attribution at the second level. Real-world data sets from water treatment systems and gas pipelines are used to evaluate the proposed model. Results show that the suggested model performs better than other rival strategies with comparable computational complexity..

1.INTRODUCTION

Cyber-physical systems (CPS) are increasingly incorporating Internet of Things (IoT) devices, including critical infrastructure sectors like dams and utility plants. IoT devices, also known as Industrial IoT (IIoT), are frequently a part of an industrial control system (ICS) in these settings, which is in charge of making sure the infrastructure runs smoothly. Systems with programmable logic controllers (PLCs) and Modbus protocols, distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems are all examples of ICS. The association between ICS or IIoT-based frameworks with public organizations, nonetheless, expands their assault surfaces and dangers of being focused on by digital aggressors. The Stuxnet campaign, which reportedly in 2010 targeted Iranian centrifuges for nuclear enrichment and severely damaged the equipment [1], [2], is one prominent example. Another model is that of the episode focusing on a siphon that brought about the disappointment of an Illinois water plant in 2011 [3]. Another campaign, BlackEnergy3, targeted Ukraine's power grids in 2015, causing approximately 230 000 people to lose power [4]. There were also reports in April

2018 of successful cyberattacks against three gas pipeline companies in the United States, which caused electronic customer communication systems to be unavailable for several days [1]. Despite their relative maturity, security solutions developed for information technology (IT) and operational technology (OT) systems may not be applicable to ICS. This could be the case, for instance, because the cyber systems and the controlled physical environment are so tightly integrated. As a result, physical behavior analysis and system availability maintenance necessitate system-level security measures [1]. In contrast to the majority of IT/OT systems, which generally prioritize confidentiality, integrity, and availability, ICS security goals are prioritized in that order [5]. Because of close coupling between factors of the criticism control circle and actual cycles, (effective) digital assaults on ICS can bring about extreme and possibly lethal ramifications for the general public and our current circumstance. This highlights the significance of developing extremely robust safety and security measures for ICS intrusion detection and prevention [1]. Signature and anomaly-based methods for attack detection and attribution are common. There have been attempts to introduce hybrid-based approaches to alleviate the known limitations of signature-based and anomaly-based detection and attribution methods [6]. Albeit crossover based approaches are successful at identifying strange enacts, they are not dependable because of continuous organization overhauls, bringing about various interruption identification framework (IDS) typologies. Beyond this, network metadata analysis (such as IP addresses, transmission ports, traffic duration, and packet intervals) is the primary component of conventional attack detection and attribution methods. As a result, machine learning (ML) or deep neural network (DNN)-based attack detection and attribution solutions have recently reawakened interest. Furthermore, assault identification approaches can be sorted into network-based or have based approaches. For the purpose of detecting attacks in network traffic, the techniques of supervised clustering, single-class or multiclass support vector machine (SVM), fuzzy logic, artificial neural network (ANN), and DNN are frequently utilized. In order to promptly identify malicious attacks, these methods analyze real-time traffic data. However, sophisticated attacks and insider attacks may be missed by attack detection that only takes into account the host and network data. Because they do not require in-depth knowledge of the cyberthreats, unsupervised models that incorporate process/physical data can enhance a system's monitoring. In general, robust security measures can be circumvented

by a sophisticated attacker with sufficient knowledge and time, such as a nation-state advanced persistent threat actor. By modeling only a system's normal behavior and reporting deviations from normal behavior as anomalies, the majority of existing methods also ignore the imbalanced property of ICS data. This is, maybe, because of restricted assault tests in existing informational collections and true situations. Even though using majority class samples is a good way to avoid problems caused by unbalanced data sets, the trained model won't be able to see the patterns in the attack samples. At the end of the day, such a methodology neglects to recognize inconspicuous assaults and experiences a high bogus positive rate [7]. Hence, there have been endeavors to use DL draws near, for instance, to work with computerized include (portrayal) figuring out how to show complex ideas from less difficult ones [8] without relying upon human-made highlights [9]. This article presents our novel two-stage ensemble deep-learning-based attack detection and attribution framework for imbalanced ICS data sets, inspired by the aforementioned observations. An ensemble representation learning model and a decision tree (DT) are used in the first stage to detect attacks in an unbalanced environment. Several one-versus-all classifiers will join together to form a larger DNN during the second stage to classify the attack attributes with a confidence interval. Additionally, the proposed framework is able to identify previously unseen attack samples. The following is a summary of our approach to this study. 1) We create a novel two-phase ensemble ICS attack detection technique that can distinguish between known and unknown attacks. In addition, we will show that, in terms of accuracy and f-measure, the proposed method performs better than other competing methods. This approach is tolerant of data with imbalances thanks to the proposed deep representation learning. 2) To reduce false alarm rates, we propose a novel self-tuning two-phase attack attribution technique that ensembles several deep one-versus-all classifiers employing a DNN architecture. Attacks with high similarity can be accurately attributed using the proposed method. This is the first ML-based assault attribution strategy in Quite a while/IIoT at the hour of this examination. 3) We examine the proposed attack detection and attack attribution framework's computational complexity to show that, despite its superior performance, it is comparable to other DNN-based methods described in the literature. The following is how the remainder of this article will be arranged:.

2.LITERATURE SURVEY

2.1 Girish L, Rao SKN (2020) "Quantifying sensitivity and performance degradation of virtual machines using machine learning.",Journal of Computational and Theoretical Nanoscience , Volume 17, Numbers 9-10, September/October 2020, pp.4055-4060(6) https://doi.org/10.1166/jctn.2020.901

Virtualized data centers bring lot of benefits with respect to the reducing the high usage of physical hardware. But nowadays, as the usage of cloud infrastructures are rapidly increasing in all the fields to provide proper services on demand. In cloud data center, achieving efficient resource sharing between virtual machine and physical machines are very important. To achieve efficient resource sharing performance degradation of virtual machine and quantifying the sensitivity of virtual machine must be modeled, predicted correctly. In this work we use machine learning techniques like decision tree, *K* nearest neighbor and logistic regression to calculate the sensitivity of virtual machine. The dataset used for the experiment was collected using collected from open stack cloud environment. We execute two scenarios in this experiment to evaluate performance of the three mentioned classifiers based on precision, recall, sensitivity and specificity. We achieved good results using decision tree classifier with precision 88.8%, recall 80% and accuracy of 97.30%.

2.2 Madala, S. R., & Rajavarman, V. N. (2018). Efficient Outline Computation for Multi View Data Visualization on Big Data. International Journal of Pure and Applied Mathematics, 119(7), 745-755

In Big data analysis, representation of data in different views with respect to visualization for handling large scale data. Continuous parallel co-ordinate framework is effective data visualization tool to analyze each attribute without any change or update in their values, without change in continues information structures and present data in structural orientation based on attributes to handle high amount of data. To present data in multi attribute evaluation, traditionally use Similarity Measure Centered with Multi Viewpoint (SMCMV) approach and related clustering approaches to represent data based on multi view data visualization procedure with different attributes. For multi dimensional and large scale data have different types of attributes to process and evaluate data based on different values in high amount of data. For efficient data processing to evaluate each attribute in separate manner to represent data in different factor with respect to returning of interest points in large scale data. So that in this paper, we present and develop

novel Hybrid machine learning with sorting algorithm to evaluate data based on different attributes with respect to interest points from high amount of data. Sorting algorithm consists two basic steps in evolution of data, first step evaluates sorted positional index, second step exploits sorted positional index and then evaluate computational with selective and sequential data into table formation. Our implemented approach performs on real world UCI repository mostly used data sets with sorting to exploit results comparison of existing algorithms with respect to time, memory and table index evaluation for sorted data.

2.3 Vivek, T. V. S., Rajavarman, V. N., & Madala, S. R. (2020). Advanced graphical-based security approach to handle hard AI problems based on visual security. International Journal of Intelligent Enterprise, 7(1-3), 250-266

Security is the main aspect to explore human data from different web oriented applications present in artificial intelligence (AI). It is very difficult to use different web applications without security to access data in various places. So that various types of security related approaches were introduced to use services in securely in outside environment, but they have some limitations to protect data from outside attackers (hackers). So that in this paper, we propose and introduce a novel and advanced security model to provide security from outside attackers in AI related web oriented applications. In this approach, we follow the basic features related to Captcha as a graphical password to enable security services in our proposed approach. Using Captcha graphical passwords in our approach, we describe pushing attacks, pass-on attacks and guessing attacks in web applications with random selection of Captcha passwords to use web services. Our experimental results show efficient security relations when compare to existing security approaches in terms of Captcha generation, time and other parameters present in web security applications

3.PROPOSEDWORK

1) We develop a novel two-phase ensemble ICS attack detection method capable of detecting both previously seen and unseen attacks. We will also demonstrate that the proposed method outperforms other competing approaches in terms of accuracy and f-measure. The proposed deep representation learning results in this method being robust to imbalanced data.

2) We propose a novel self-tuning two-phase attack attribution method that ensembles several deep one-versusall classifiers using a DNN architecture for reducing false alarm

rates. The proposed method can accurately attribute attacks with high similarity. This is the first ML-based attack attribution method in ICS/IIoT at the time of this research.

3) We analyze the computational complexity of the proposed attack detection and attack attribution framework, demonstrating that despite its superior performance, its computational complexity is similar to that of other DNN-based methods in the literature.

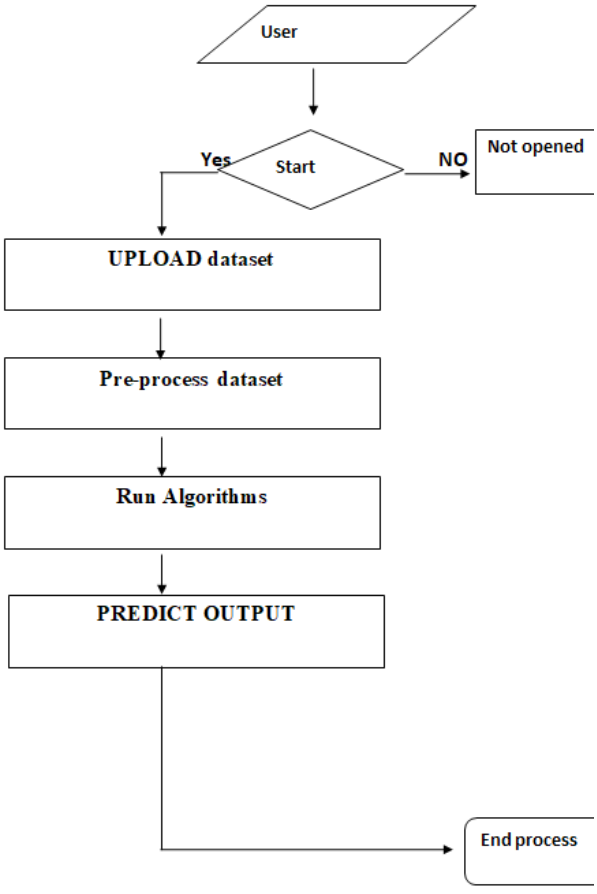

Fig 1:Working Architecture

3.1 IMPLEMENTATION

3.1.1 Upload SWAT Water Dataset: using this module we will upload dataset to application and then read dataset and then find different attacks found in dataset

3.1.2 Preprocess Dataset: using this module we will replace all missing values with 0 and then apply MIN-MAX scaling algorithm to normalized features values and then split dataset into train and test where application used 80% dataset for training and 20% for testing

3.1.3 Run AutoEncoder Algorithm: using this module we will trained AutoEncoder deep learning algorithm and then extract features from that model.

3.1.4 Run Decision Tree with PCA: extracted features from AutoEncoder will get transform using PCA to reduce features size and then retrain with Decision tree. Decision tree will predict label for each record based on dataset signatures

3.1.5 Run DNN Algorithm: predicted decision tree label will further train

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

with DNN (deep neural network) algorithm to detect and attribute attacks

3.1.6 Detection & Attribute Attack Type: using this module we will upload unknown or un-label TEST DATA and then DNN will predict attack type

3.1.7 Comparison Graph: using this module we will plot comparison graph between all algorithms

4.RESULTS AND DISCUSSION

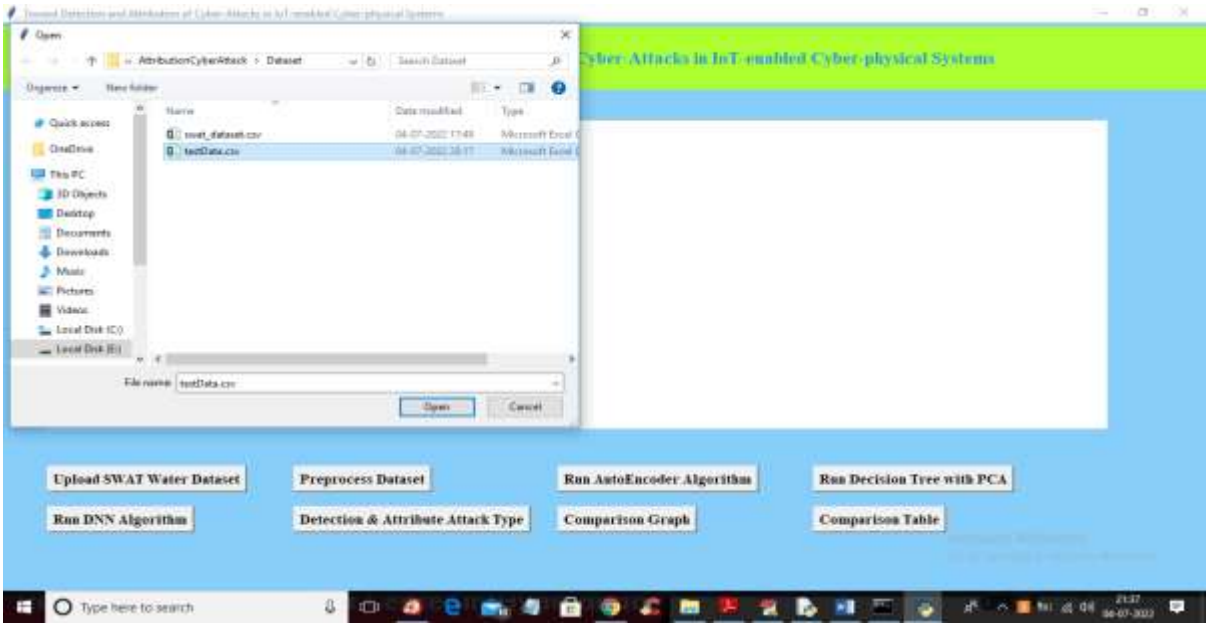

Fig 2:In above screen selecting and uploading 'TEST DATA' file and then click on 'Open' button to get below output

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

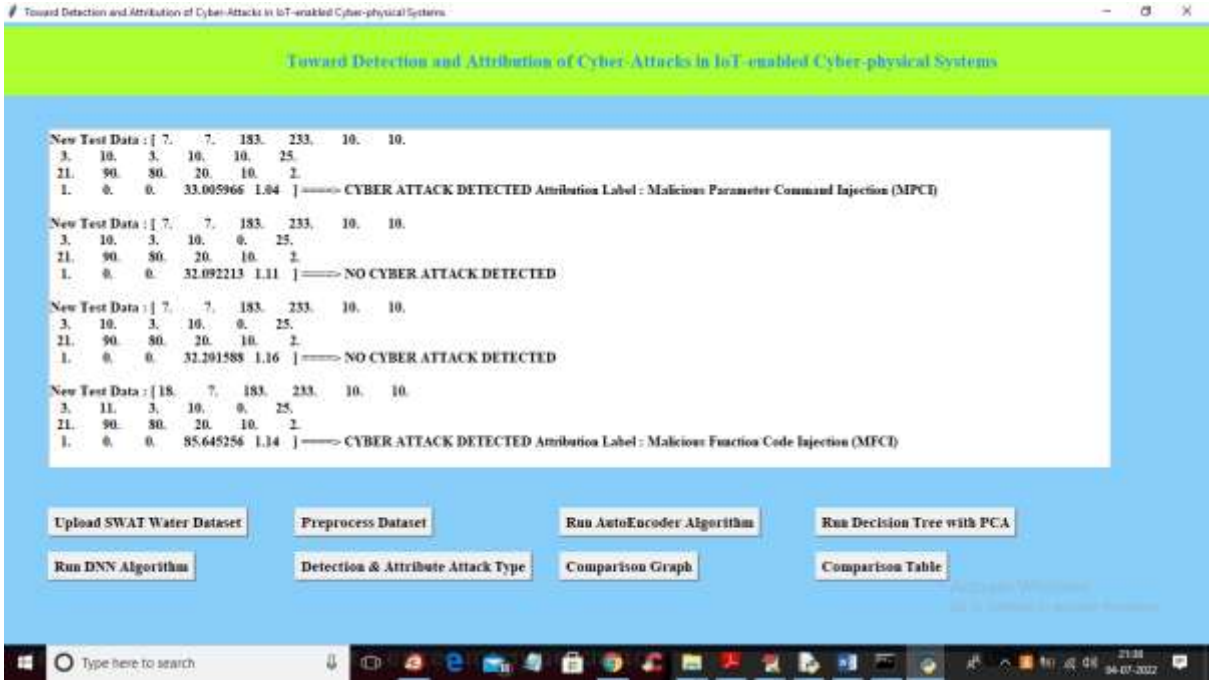

Fig 3:In above screen we can see detected various attacks and now click on 'Comparison Graph' button to get below graph

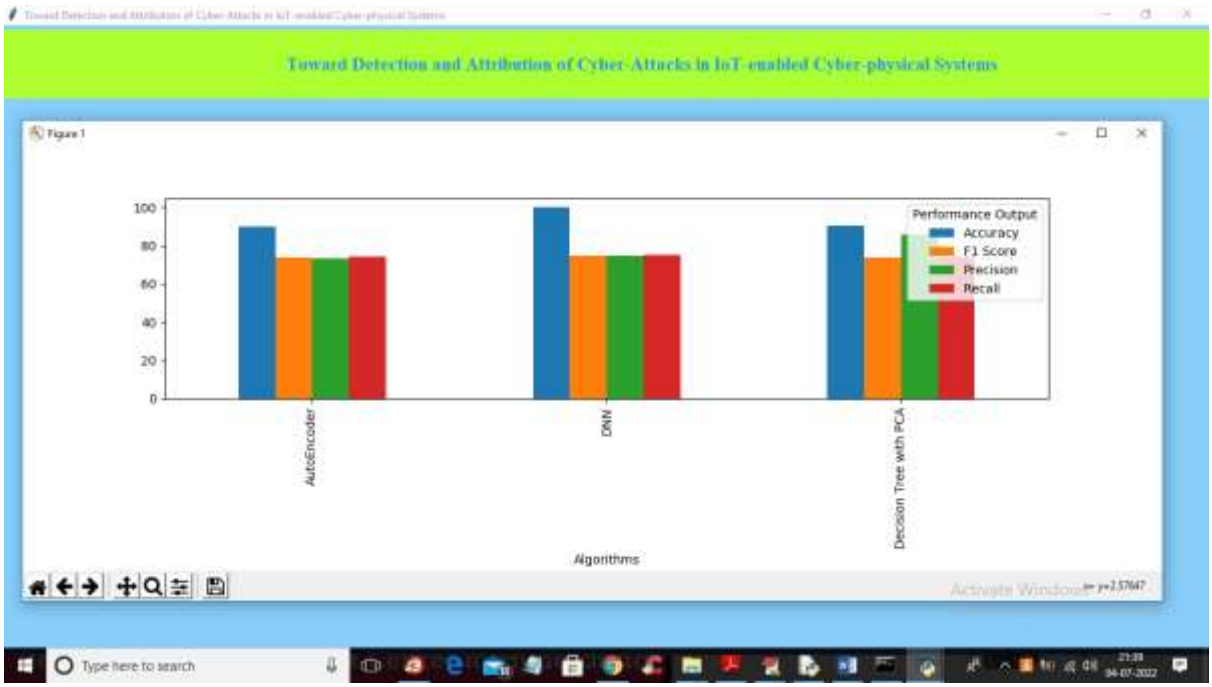

Fig 4:In above graph x-axis represents algorithms names and y-axis represents different metric values such as precision, recall, accuracy and FSCORE with different colour bars and in all algorithms DNN got high accuracy and now close above graph and then click on 'Comparison Table' to get below comparison table of all algorithms

5.CONCLUSION

Cyber-physical systems (CPS) that are Internet of Things (IoT) enabled can be difficult to secure because security measures designed for general information/operational technology (IT/OT) systems may not work as well in a CPS environment. Thus, a two-level ensemble attack detection and attribution framework for CPS—and more specifically, an industrial control system (ICS)—is presented in this article. For detecting attacks in unbalanced ICS environments, a decision tree combined with a novel ensemble deep representation-learning model is developed at the first level. An ensemble deep neural network is created to facilitate attack attribution at the second level. Real-world data sets from water treatment systems and gas pipelines are used to evaluate the proposed model. Results show that the suggested model performs better than other rival strategies with comparable computational complexity.

REFERENCES

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.

[2] R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001.

[3] M. Baykara, R. Das¸, and I. Karado ˘gan, "Bilgi g ¨uvenli ˘gi sistemlerinde kullanilan arac¸larin incelenmesi," in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.

[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.

[6] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with lda and pca," in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[7] N. Moustafa and J. Slay, "The significant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems," in Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.

[8] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using benford's law," in Asia-Pacific Signal and Information Processing

Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.

[9] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.

[10] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5

Author's Profiles

PVN Rajeswari has received her B.Tech in CSE from Andhra University and M.Tech in CSE from Allahabad University in 2004 and in 2006 respectively. She submitted her PhD thesis to Andhra University in 2023 and she is dedicated to teaching field from 2006. She has guided 20 P.G and 48 U.G projects. Her research areas are Security, Artificial Intelligence and Machine learning. At present she is working as Associate Professor in PBR VITS, Kavali, Andhra Pradesh, India.

V VARSHITHA B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute Of Technology & Science, Kavali.

S MINALI B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute Of Technology & Science, Kavali.

R LAKSHMI LIKHITHA B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute Of Technology & Science, Kavali.

M VINEELA B.Tech with Specialization of Computer Science and Engineering in PBR Visvodaya Institute Of Technology & Science, Kavali.