ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.03
October-2023
Pages: 968-978

A NEW TOWARD DETECTION AND ATTRIBUTION OF CYBER-ATTACKS IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

*** Mr. PRAVEEN KUMAR**
*Asst. Professor, Dept. of CSE, **MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, TELANGANA, INDIA
M. KOKILA REDDY[1], M. NAVYA SRI[2], M. SRIJA[3], N. VAISHNAVI[4]
B. Tech Pursuing, Dept. of CSE**, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN**, TELANGANA, INDIA

ABSTRACT

Internet of Things enabled cyber bodily structures such as Industrial equipment's and operational IT to ship and get hold of information over internet. This equipment's will have sensors to feel gear situation and document to centralized server the usage of web connection. Sometime some malicious customers can also assault or hack such sensors and then alter their statistics and this false statistics will be file to centralized server and false motion will be taken. Due to false facts many nations gear and manufacturing gadget obtained failed and many algorithms used to be developed to notice assault however all these algorithms go through from statistics imbalance (one category my carries massive data (for instance NORMAL data and different type like assault may additionally includes few files which lead to imbalance trouble and detection algorithms can also failed to predict accurately). To deal with records imbalance current algorithms have been the usage of OVER and UNDER sampling which will generate new documents for FEWER class, however this method enhance accuracy however now not up to the mark.To overcome from this issue, we are introducing novel method besides the use of any underneath or oversampling algorithms and this method consists of two components

1. INTRODUCTION

The large-scale growth of the Internet of things (IoT) in recent years has contributed to a significant increase in fog computing, smart cities, and Industry 4.0, all of which execute the complex data processing of confidential information that must be protected against cybersecurity attacks. Cybersecurity attacks have increased rapidly in various domains, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes. As a result of their wide range of services, IoT device sensors generate large amounts of data that requires authentication, security, and privacy. Previously, traditional methods and frameworks were used to ensure the security of IoT. However, the application of

different artificial intelligence (AI) methods for detecting cybersecurity attacks has gained in popularity over the years. IoT comprises interconnected devices that are increasingly developed on a large scale, taking into account various characteristics through cloud and fog computing, where the processing of real-time applications can be enhanced. Cyber-physical systems (CPSs) are integrated technologies such as healthcare IoT, industrial IoT (IIoT), smart cities IoT, AI and big data, that are part of the fourth industrial revolution (Industry 4.0), and are used for innovation in smart industries to promote data transmission between networks. To overcome the security issues that threaten the IoT, several researchers have developed IDSs based on various AI approaches. Kurte et al. for example, introduced a distributed service framework that supports the development of trustworthiness and privacy protection for multi directional data aggregation for edge computing enhancement. Diro and Chilamkurti proposed a detection system using deep learning (DL) methods to detect cybersecurity attacks in IoT. They compared the DL model with traditional machine learning (ML) approaches. Farivar et al. identified AI for the detection of malicious attacks in CPS and IIoT and proposed a hybrid intelligent classic control approach for the reconstruction of cyberattacks on the input data of non-linear CPS through shared networks. Security in the IoT requires additional considerations to protect connected smart devices from threats and other vulnerabilities using effective AI techniques towards monitoring. In addition, IoT security systems are designed using AI enhanced encryption algorithms to archive privacy. For example, Obaidat et al. investigated in-depth IoT attacks, threats and vulnerability through classification based on severity impact, also providing a multi-faceted method to countermeasure those security concerns. Li et al. proposed a novel privacy prevention of ML training with classification process through a security framework based on a homomorphic encryption scheme over a matrix ring, which also supports ciphertexts homomorphic comparison. Sarica and Angin provided explainable security in IoT networks by proposing a real-time automated intrusion detection approach using ML classifiers in software-defined networking (SDN) application layer to detect an attack. Aleem et al. provide security concerns for data warehouse (DWH) with each type of security approach. Furthermore, it includes a new and unique CPS if the countermeasure is insufficient. Patil et al. proposed a virtual machine-assisted lightweight agent-based malware detection framework for securing a virtual machine in cloud computing, while, Dang et al. proposed an authentication method for securing cloud servers in IoT environments.

2. LITERATURE PREVIEW

1) Theoretical foundations of automated control

AUTHORS: Tarek Abdelzaher1 , Yixin Diao2 , Joseph L. Hellerstein3 , Chenyang Lu4 , and Xiaoyun Zhu

We consider the problem of planning the ISS cosmonaut training with different objectives. A pre-defined set of minimum qualification levels should be distributed between the crew members with

minimumtraining time differences, training expenses or a maximum of the train-ing level with a limitation of the budget.First, a description of the cosmonaut training process is given.Then four models are considered for the volume planning problem.The objective of the first model is to minimize the differences between the total time of the preparation of all crew members, the objective of the second one is to minimize the training expenses with a limitation of the training level, and the objective of the third one is to maximize the training level with a limited budget. The fourth model considers the problem as an n -partition problem. Then two models are considered for the calendar planning problem.We consider the problem of planning the ISS cosmonaut training with different objectives. A pre-defined set of minimum qualification levels should be distributed between the crew members with minimum training time differences, training expenses or a maximum of the train-ing level with a limitation of the budget. First, a description of the cosmonaut training process is given. Then four models are considered for the volume planning problem.The objective of the first model is to minimize the differences between the total time of the preparation of all crew members, the objective of the second one is to minimize the training expenses with a limitation of the training level, and the objective of the third one is to maximize the training level with a limited budget. The fourth model considers the problem as an n -partition problem. Then two models are considered for the calendar planning problem

Abstract: We consider the problem of planning the ISS cosmonaut trainingwith different objectives. A pre-defined set of minimum qualification levels should be distributed between the crew members with minimum training time differences, training expenses or a maximum of the train-ing level with a limitation of the budget.

First, a description of the cosmonaut training process is given.Then four models are considered for the volume planning problem.The objective of the first model is to minimize the differences between the total time of the preparation of all crew members, the objective of the second one is to minimize the training expenses with a limitation of the training level, and the objective of the third one is to maximize the training level with a limited budget. The fourth model considers the problem as an n -partition problem. Then two models are considered for the calendar planning problem

Abstract: We consider the problem of planning the ISS cosmonaut training with different objectives. A pre-defined set of minimum qualification levels should be distributed between the crew members with minimum

training time differences, training expenses or a maximum of the train-ing level with a limitation of the budget.

First, a description of the cosmonaut training process is given.Then four models are considered for the volume planning problem.

The objective of the first model is to minimize the differences between the total time of the preparation of all crew members, the objective of the second one is to minimize the training expenses with a limitation of the training level, and the

objective of the third one is to maximize the training level with a limited budget. The fourth model considers the problem as an n-partition problem. Then two models are considered for the calendar planning problem

Feedback control is central to managing computing systems and data networks. Unfortunately, computing practitioners typically approach the design of feedback control in an ad hoc manner. Control theory provides a systematic approach to designing feedback loops that are stable in that they avoid wild oscillations, accurate in that they achieve objectives such as target response times for service level management, and settle quickly to their steady state values. This paper provides an introduction to control theory for computing practitioners with an emphasis on applications in the areas of database systems, real-time systems, virtualized servers, and power management.

We consider the problem of planning the ISS cosmonaut trainingwith different objectives. A pre-defined set of minimum qualification levels should be distributed between the crew members with minimum training time differences, training expenses or a maximum of the train-ing level with a limitation of the budget.First, a description of the cosmonaut training process is given.

Then four models are considered for the volume planning problem.The objective of the first model is to minimize the differences between the total time of the preparation of all crew members, the objective of the second one is to minimize the training expenses with a limitation of the training level, and the objective of the third one is to maximize the training level with a limited budget. The fourth model considers the problem as an n-partition problem. Then two models are considered for the calendar planning problem.For the volume planning problem, two algorithms are presented.The first one is a heuristic with a complexity of (n)operations. The second one consists of a heuristic and exact parts, and it is based on the n-partition problem approach.

2) Application of Artificial Intelligence Systems in the Process of Crew Training

AUTHORS: Andrey Kuritsyn FBSO “Yu. A. Gagarin Research&Test Cosmonaut Training Center”, Moscow, Russia,Maxim Kharlamov FBSO “Yu. A. Gagarin Research&Test Cosmonaut Training Center”, Moscow, Russia,Sergei Prokhorov S.I. Vavilov Institute for the History of Science and Technology of the RAS, Moscow Institute of Physics and Technology, Moscow, Russia,Dmitry Shcherbinin S.I. Vavilov Institute for the History of Science and Technology of the RAS, Moscow, Russia

The article considers the issues of managing the process of integrated training of orbital space station crews in the context of conversion to advanced digital smart technologies, computer-assisted training and artificial intelligence. The proposed approach is based on the use of automated information systems to support the planning and management of crew training on integrated and special-purpose simulators using an artificial intelligence technology.

3. EXISTING SYSTEM:

The existing system for detecting and attributing cyber-attacks in IoT-enabled Cyber-physical Systems (CPS) typically

relies on a combination of intrusion detection systems (IDS), network traffic monitoring, and anomaly detection techniques. These systems are designed to identify unusual or suspicious activities within the network, indicating a potential cyber-attack. They may use signatures of known attacks, heuristics, or machine learning algorithms to analyze network traffic patterns.

DISADVANTAGES:

- However, in many cases, the existing systems face challenges when it comes to accurately attributing cyber-attacks to specific entities or sources.
- They often struggle to provide concrete evidence of the attacker's identity, intention, or origin. This is due to factors such as the use of anonymizing technologies, sophisticated attack strategies, and the rapid evolution of attack vectors.

4. PROPOSED SYSTEM

The proposed system aims to enhance the existing methods for detecting and attributing cyber-attacks in IoT-enabled CPS by incorporating advanced techniques and technologies. The key innovations and improvements include:

1. Advanced Machine Learning Algorithms:

Utilizing state-of-the-art machine learning models, such as deep learning algorithms, for improved anomaly detection and attack attribution. These models can learn complex patterns and behaviors, making them more adept at identifying subtle indications of cyber-attacks.

2.Behavioral Profiling:

Creating comprehensive behavioral profiles for devices and entities within the CPS network. This involves analyzing normal behavior patterns of devices, users, and processes to establish a baseline. Deviations from this baseline can be flagged as potential security incidents.

3.Contextual Analysis:

Incorporating contextual information, such as device location, time of day, user behavior, and network topology, to enrich the analysis. This helps in distinguishing between legitimate activities and suspicious behavior.

4. Forensic Data Collection:

Implementing robust data logging and forensics capabilities to capture detailed information about network activities. This includes logging network traffic, system events, and interactions between devices.

ADVAVANTAGES

Threat Intelligence Integration:Integrating threat intelligence feeds and databases to cross-reference detected anomalies with known attack patterns and tactics used by cyber criminals.

Blockchain for Attribution:Leveraging blockchain technology to create immutable records of network activities. This can aid in preserving the integrity and authenticity of the attribution data, making it harder for attackers to manipulate or conceal their tracks.

Collaborative Security Frameworks:

Facilitating information sharing and collaboration among various entities within

the IoT ecosystem, including device manufacturers, service providers, and security experts. This collective effort can enhance the collective defense against cyber-attacks.

Legal and Regulatory Considerations:

Addressing legal and regulatory frameworks for cyber-attack attribution, ensuring compliance with data privacy laws while enabling effective attribution.

By combining these advancements, the proposed system aims to significantly improve the accuracy and reliability of cyber-attack detection and attribution in IoT-enabled CPS environments. It seeks to provide a more comprehensive understanding of cyber threats, enabling faster response times and better protection of critical infrastructure.

Auto Encoder: auto encoder deep learning will get trained on imbalanced dataset and then extract features from it and this extracted featured will get trained with DECISION TREE algorithm to predict label for known or unknown attacks. Decision tree get trained on reduced number of features obtained from PCA (principal component analysis) algorithm.

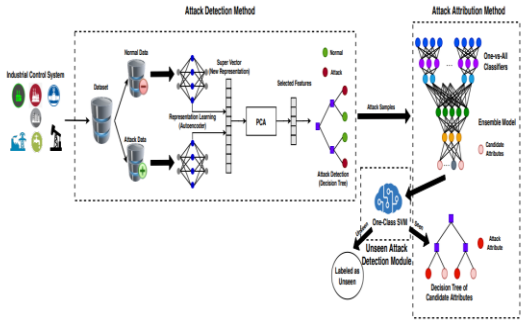
Deep Neural Network (DNN): in this level DNN algorithm get trained on known and unknown attacks. If any records contain attack signature, then DNN will identify attack label or class and attribute them.

To implement this project, we have used SWAT (secure water production treatment) and this dataset contains IOT request and response signature and associate each dataset with unique attack label and dataset contains below cyber-attack labels

'Normal', 'Naive Malicious Response Injection (NMRI)', 'Complex Malicious', 'Response Injection (CMRI)', 'Malicious State Command Injection (MSCI)', 'Malicious Parameter Command Injection (MPCI)', 'Malicious Function Code Injection (MFCI)', 'Denial of Service (DoS)'

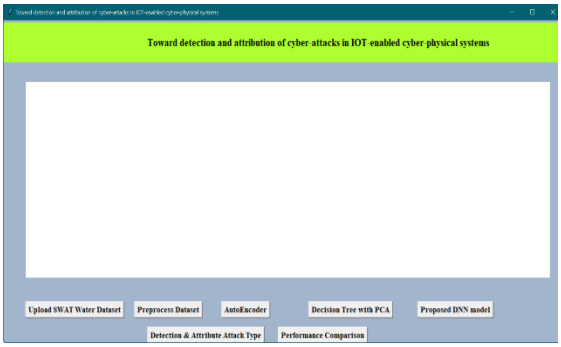
Above are the attacks found in dataset and dataset contains above labels as integer value of its index for example NORMAL label index will be 0 and continues up to 8 class labels. Below screen showing dataset details.

5. SYSTEM ARCHITECTURE

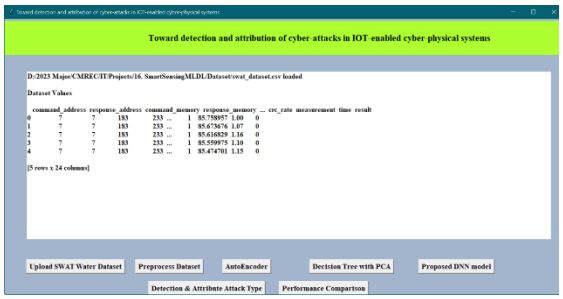


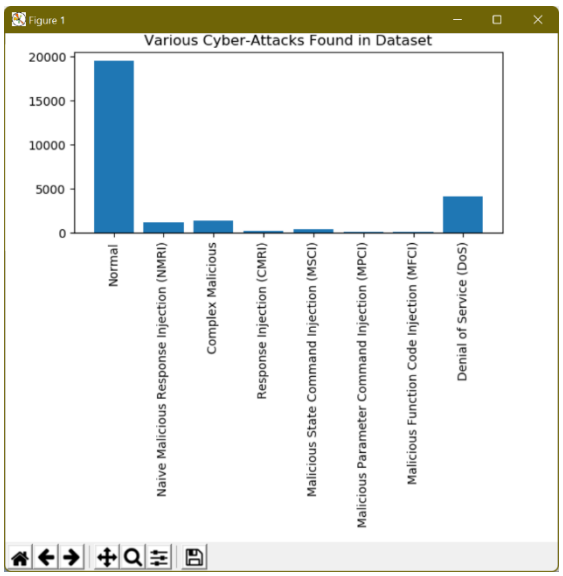
6. RESULT

To run project double click on 'run.bat' file to get below screen



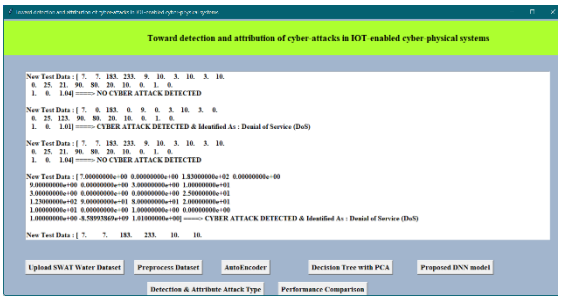
In above screen click on 'Upload SWAT Water Dataset' button to upload dataset to application and get below output In above screen selecting and uploading SWAT dataset file and then click on 'Open' button to load dataset and get below output





In above screen dataset loaded and in graph x-axis contains ATTACK NAME and y-axis contains count of those attacks found in dataset and we can see 'NORMAL' class contains so many records and other attacks contains very few records so it will raise data imbalance problem which can be solved using AutoEncoder, Decision Tree and DNN. Now close above graph and then click on 'Preprocess Dataset' button to remove missing values and then normalized values with MIN-MAX algorithm all values are normalized (converting data between 0 and 1 called as normalization) and then we can see total records in dataset and then dataset train and test split records count also displaying. Now dataset is ready and now click on 'AutoEncoder' button to train dataset with AutoEncoder and get below accuracy.

In above screen with AutoEncoder we got 90.18% accuracy, and this accuracy can be enhance by implementing Decision Tree with PCA algorithm and now click on 'Decision Tree with PCA' button to get below output this accuracy may vary from 95 to 100% as we are splitting dataset into random train and test. Now click on 'Detection & Attribute Attack Type' button to upload test DATA and detect attack attributes uploading 'TEST DATA' file and then click on 'Open' button to get below output.



In above screen in square bracket, we can see TEST data values and after arrow =➔

symbol we can see detected ATTACK TYPE and scroll down above text area to view all detection.

In above screen we can see detected various attacks and now click on 'Performance Comparison' to get below comparison table of all algorithms

Algorithm Name	Accuracy	Precision	Recall	FSCORE
AutoEncoder	90.0	73.14281070224018	73.58689458689459	73.29616654463219
Decision Tree with PCA	90.47794117647706	85.75313833952161	74.62748067246231	73.96952834086689
DNN	100.0	100.0	100.0	100.0

In above table we can see algorithm names and its metrics values such as accuracy and precision and other.

7. CONCLUSION

In this paper, we present a systematic review of cybersquatting detection attacks in the IoT using AI methods. Due to their rapid development in the various domains, large amounts of data are constantly being generated, which requires an increased focus on privacy and security. Attacks in IoT can be categorized into Probe, R2L, U2R, and DoS. If these attacks succeed, IoT performance can be compromised in many ways such as giving false information. While in the past, traditional methods have been used for improving IoT security, due to the rapid evolution of cyber threats. As a result of industrial 4.0, the AI approach can be considered one of the most promising methods.

8. REFERENCES

1. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the Next Generation Networks and Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3515–3520. [CrossRef]

2. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* **2020**, *101*, 102031. [CrossRef]

3. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. *Futur. Gener. Comput. Syst.* **2022**, *127*, 286–296. [CrossRef]

4. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. *Sustain. Cities Soc.* **2021**, *75*, 103311. [CrossRef] [PubMed]

5. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4166–4176. [CrossRef]

6. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and

multidirectional data aggregation for edge computing

enhanced IoT. *J. Syst. Archit.* **2020**, *106*, 101713. [CrossRef]

7.Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]

8. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2716–2725. [CrossRef]

9. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]

10. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. *Electronics* **2020**, *9*, 2152. [CrossRef]

11. Zhang, T.; Zhao, Y.; Jia, W.; Chen, M.Y. Collaborative algorithms that combine AI with IoT towards monitoring and control system. *Futur. Gener. Comput. Syst.* **2021**, *125*, 677–686. [CrossRef]

12.Li, B.; Feng, Y.; Xiong, Z.; Yang, W.; Liu, G. Research on AI security enhanced encryption algorithm of autonomous IoT systems. *Inf. Sci.* **2021**, *575*, 379–398. [CrossRef]

13. Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet Things* **2021**, *15*, 100420. [CrossRef]

14. Obaidat, M.A.; Obeidat, S.; Holst, J.; Hayajneh, A.A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]

15. Li, J.; Kuang, X.; Lin, S.; Ma, X.; Tang, Y. Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. *Inf. Sci.* **2020**, *526*, 166–179. [CrossRef]

16. Sarica, A.K.; Angin, P. Explainable security in SDN-based IoT networks. *Sensors* **2020**, *20*, 7326. [CrossRef] [PubMed]

17. Aleem, S.; Capretz, L.F.; Ahmed, F. Security Issues in Data Warehouse. *arXiv* **2015**, arXiv:1507.05644.

18. Wu, M.; Song, Z.; Moon, Y.B. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods.

J. Intell. Manuf. **2019**, *30*, 1111–1123. [CrossRef]

19. Patil, R.; Dudeja, H.; Modi, C. Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing. *Int. J. Inf. Secur.* **2020**, *19*, 147–162. [CrossRef] 20. Dang, T.K.; Pham, C.D.M.; Nguyen, T.L.P. A pragmatic elliptic curve cryptography-based extension for energy-efficient device-todevice communications in smart cities. *Sustain. Cities Soc.* **2020**, *56*, 102097. [CrossRef]

21.Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets.*Sustain. Cities Soc.* **2021**, *72*, 102994. [CrossRef]

22. Atul, D.J.; Kamalraj, R.; Ramesh, G.; Sakthidasan Sankaran, K.; Sharma, S.; Khasim, S. A machine learning based IoT for providing an intrusion detection system for security. *Microprocess. Microsyst.* **2021**, *82*, 103741. [CrossRef]

23. Ghosh, A.; Chakraborty, D.; Law, A. Artificial intelligence in Internet of things. *CAAI Trans. Intell. Technol.* **2018**, *3*, 208–218. [CrossRef]

24. Bland, J.A.; Petty, M.D.; Whitaker, T.S.; Maxwell, K.P.; Cantrell, W.A. Machine Learning Cyberattack and Defense Strategies. *Comput. Secur.* **2020**, *92*, 101738. [CrossRef]

25. Rathore, S.; Park, J.H. Semi-supervised learning based distributed attack detection framework for IoT. *Appl. Soft Comput. J.* **2018**, *72*, 79–89. [CrossRef] .

AUTHOR

Mr.Praveen kumar Assistant Professor Department of CSE MallaReddy Engineering College for Women, pshiremath017@gmail.com Hyderabad,