ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

Cyber Attack Detection in Smart Agriculture Data Using Machine Learning Approaches

*Dr. S. V. Saboji [1] , Suresh Talwar [2]

[1]Professor, Basaveshwar Engineering College, Bagalkot-587104

[2]Assistant Professor, St. Martin's Engineering College, Secunderabad, Telangana – 500100

*Corresponding Author

Email: sabojiskumar@yahoo.com

Abstract :A significant amount of potentially sensitive data may be leaked from sensors put everywhere in the internet in an Internet of Things(IoT) environment, It is crucial to first confirm the data source IOT system is IoT device identification environment. It is crucial to first confirm the data's source and identity in order to assure the veracity of such sensitive material. Practically speaking, the first step to a secure IoT system is IoT device identification. In critical or emergency scenarios, harmful behaviors like providing erroneous data that cause irreparable security issues can be stopped by using the right device identification approach. According to recent study, because of their instability or accessibility, primary identity metrics like Internet Protocol (IP) or Media Access Control (MAC) addresses are insufficient. As a result, it is crucial to take into account how to analyze sensor and packet header information to identify an IoT device. This article suggests a framework for device identification based on classification using combination of sensor measurement and a packet header data set. In order to provide improved security in IoT devices, various machine learning methods have been implemented to identify anomaly. Data gathered from IoT devices has been used to test the suggested technique under attack conditions.

Keywords: IoT security, Smart agriculture, Machine learning, Anomaly detection

1. Introduction

Every day, smart agriculture emerges to address issues including climate change, resource waste, excessive pesticide use, and low agricultural productivity. In particular, the term "sustainability" has historically been associated with industry and agriculture because of their efforts to lessen the environmental impact of their operations. The advantages of this method are inextricably tied to the accuracy and availability of meteorological, soil, crop, and climate data, as well as their quality and suitability for use in production. The Internet of Things (IoT) paradigm[20], which is defined as a significant number of heterogeneous devices, technologies, and protocols connected to the Internet, emerges as an alternative. As a result of the widespread use of IoT, affordable devices are now a competitive alternative for sensing urban surroundings. Information technology, which is widely employed in business, environmental monitoring, and other areas of life, can significantly contribute to the development of the rural economy. The majority of farmers use excessive amounts of water that reduce soil fertility because they are unaware of how much water is needed for the plants. Precision agriculture[19], which is the application of

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

innovative technologies to boost agricultural productivity, helps provide farmers with all the current and trustworthy information they need.

In order to develop crops, increase agricultural production, and assist farmers in becoming more effective, smart agriculture [1] is essential. It helps farmers achieve appropriate irrigation to prevent water waste, minimize soil fertility, improper fertilizer use, and disease. Wireless farming sensors are installed in agricultural areas to gather data from the environment and safely transmit it to the base station in order to make informed decisions. These sensors can extract information about the composition of the soil, including humidity, temperature, humidity levels, and water level detectors. The Internet of Things has been used to provide a system for monitoring environmental parameters. Changes in climate parameters will be tracked by the system. The system primarily consists of switches, a central node (gateway), and field-installed nodes. Field data is measured by the sensor attached to the sensing node and transferred in a single or several hops to the gateway. Using the 4G/LTE network, the central node collects field data from the sensor nodes, retrieves weather data, and transmits miniature records to the central server.

2. Literature review

In a nation that is dealing with severe food insecurity issues, population expansion, climate change, resource depletion, significant food waste, and restrictions brought on by pandemics like COVID-19, using digital technologies in food production is a realistic alternative for achieving food security. Precision agriculture and the agri-food supply chain are used to digitise the agricultural food production process as part of agriculture 4.0, the fourth industrial revolution in agriculture [2]. IoT, big data/cloud computing, block chain technology, AI, robots, autonomous cars, additive manufacturing, AR/VR, sustainable packaging, cellular agriculture, and other technologies are among the ten enabling technologies for agriculture 4.0.

A key component of secure IoT systems is mutual authentication between IoT servers and devices. Widely used single password authentication techniques are susceptible to side-channel and dictionary attacks. Present a multi-key (or multi-password) based mutual authentication mechanism in the paper [3]. This method uses a secure vault, which is a group of keys of similar sizes, as the intermediary between the Internet of Things server and the Internet of Things device. The secure vault's initial contents are shared between the server and the IoT device, and they are updated following each successful communication session. Safe from side channel attacks used to compromise the IoT devices' security.

For unbalanced industrial control system (ICS) data, this paper's [4] innovative two-stage ensemble deep learning-based attack detection and attack attribution architecture was suggested. The attack detection stage applies a DT to identify the attack samples after mapping the samples to the new higher dimensional space using deep representation learning. IoT botnet assaults can be prevented and detected using a two-pronged machine learning strategy [5]. We trained a cutting-edge deep learning model in the first fold. The ResNetDDoS-1 model was trained in the second fold to identify DDoS attacks in the event that the scanning detection model is unable to stop a botnet attack. Additionally, the experimental findings demonstrated that the ResNetScan-1 and ResNetDDoS-1 models outperformed all other models for detecting scan and DDoS attacks. Therefore, the suggested two-fold approach is effective and reliable to stop and identify IoT botnet attacks with a wide coverage of attack patterns.

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

Because control Centre's and people are typically geographically separated, cyber attacks on sensor measurements may result in the loss of user privacy, information, and trust. This motive is what spurred the paper[6] suggestion of an IoT-based method for estimating human movements in the face of cyber attacks. The sensing measures are sent to the control Centre via a faulty communication link, which is also the site of a cyber attack. The ideal state estimation algorithm is created to estimate human motions based on mean squared error.

The cyber-physic system (CPS) in Industry 4.0 serves as the foundation for the proposed IoT architecture [7],[8]. The deployment of IoT topology for the online monitoring and tracking of the GIS status, however, faces significant obstacles from cyber attacks and the classification of GIS insulation problems. Advanced machine learning algorithms are used to conduct the paradigm and verification in order to detect cyber-attacks..

The suggested method [9] combines artificial neural networks and nonlinear control. To ensure the stability and resilience of the cyber-physical systems (CPS), nonlinear control theory is used. Based on the adaptation law discovered by the Lyapunov stability proof, which in turn ensures the stability of the closed-loop controlled CPS, learning of the NN estimator is employed for attack estimate. Adept, a distributed framework to detect and identify the distinct attack stages of a coordinated attack, is presented in the paper [14][15]. Three stages make up Adept's process. IoT device network traffic is first examined locally to look for anomalies compared to their normal characteristics. Any alert associated with a possible anomaly is forwarded to a security manager, where aggregated alerts are mined using frequent item set mining (FIM) to look for patterns that are correlated over both time and space. Finally, it uses a machine learning approach to distinguish between individual attack stages in the generated alerts by using both alert-level and pattern-level information as features.

3. System Model

IoT devices are being included into smart agriculture all around the world, which has led to a rise in sophisticated cyber attacks that coordinate diverse attacks from many locations. As a result, more sophisticated systems are needed for vulnerability assessments and cyber attack detection. We took into account the simulated data in order to accurately identify the vulnerabilities. In other words, a genuine synthetic attack scenario would be developed on the simulation network in order to identify any potential weaknesses. We looked into machine learning methods that would produce the best results for identifying Cyber attacks. In this study, we take into account potential remote access attack scenarios in IOT systems that un-trusted device identification method can work on. We aim to demonstrate that our model can detect attacks coming from the fault device by using a classification mechanism using machine learning techniques in addition to identifying the identity of the device.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

the temperature and humidity, which could result in a critical occurrence in settings like hospitals that call for cautious consideration.

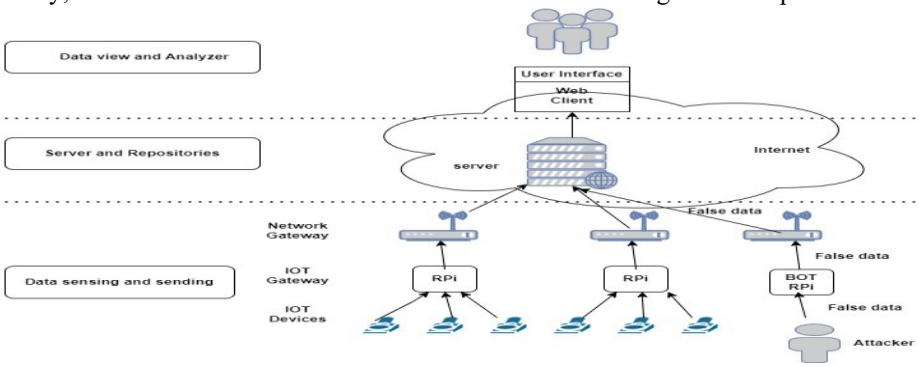

Figure 1: Botnet attack model

4. Intrusion detection Framework-

The framework, which decides on device identity by automatically classifying fault devices as Intruder, is shown in high-level in Figure 2. Such classification relies on sensor readings, IP address and MAC address of Device, and a classifier model to function. This framework consists of data collecting; dimension extraction, analytical engine, and security management are the four layers that make up the overall structure. The Model Management and Security Management modules are two more important components of the system. Model Management will be performing the best features extraction and analyzing their value or weight using ML techniques. Security Management chooses the security options for identifying Intruder, including whether or not it is attack happened, and offers the enforcement assistance after the dimensions have been extracted and the ML model of the Intrusion detection has been determined.

Two databases (DBs) are also available for managing the data. The sensor measurements details, and address names are all contained in the first database, called Sensor and Header DB. The values for each dimension will be elicited from the observation after the necessary dimensions have been loaded from the first DB, and the trained model will then be saved in the Classifier DB.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

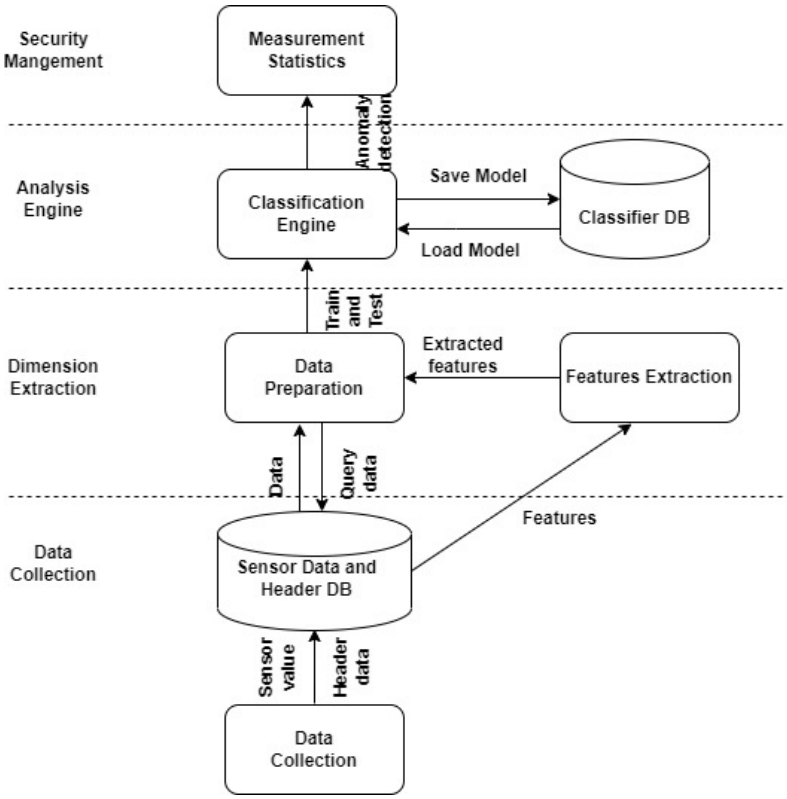

Figure 2 Framework for Identification of Intrusion detection in Smart Agriculture the start of the Data Collection layer, this data-driven framework is gathered from sensor devices via GPS (Global Positioning System), Wi-Fi, and Bluetooth. A packet analyzer like Pyshark simultaneously records the traffic features taken from packet headers. Then, based on the value of the extracted features, the Features Extraction module applies all the features to calculate the feature vector to characterize the current observation.

The Data Preparation module will then send a data query to Sensor and Header DB to locate the required sensor and header data. Using a training and testing set, the sensor data and extracted characteristics are trained to create the Intrusion detection model during the learning phase. The trained model from the Classification Engine is kept in the Classifier DB.

5. Enforcement

The implementation details consist of system methodology and steps, model creation and Selection, and feature extraction are presented as follows.

5.1 Methodology

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

To describe the device identification framework, Figure 3 depicts a workflow of implementation steps. As seen in the figure, the firta step in implementing the device identification framework is to setup the environmental modules includes: node module, IoT gateway and sensors connected to IoT gateways. All the modules will be operated over the server. All these modules generate a concrete security module that is easy to plug-in on various servers, due to its modularity.

Once all the required modules are running, in the Data capturing and preparation step, the sensor measurements can be stored in the sensor-DB. Simultaneously, header information related to HTTP messages arriving from the sensors can be captured and extracted to the header-DB.

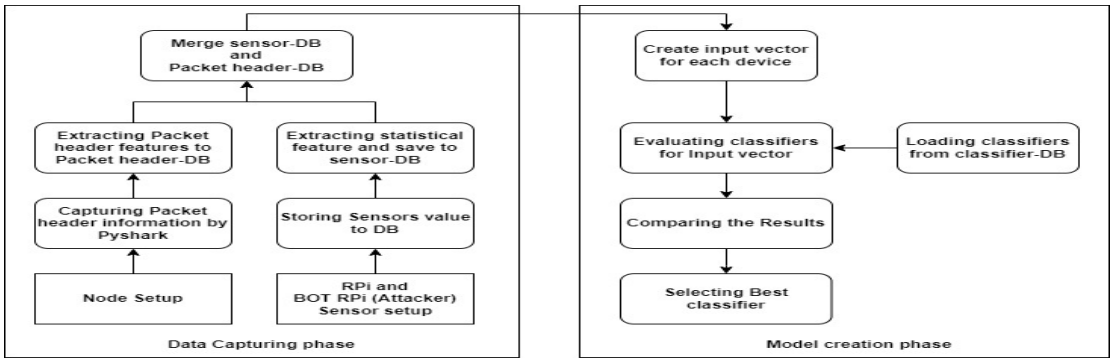

Figure 3: Model Creation Steps

Alongside the sensor measurements and header features, few smart agriculture features for cultivation of crop are stored based on the different interval of date-time which will be stored in sensor-DB. Therefore, for each sensor data sent to the server, two categories of features (sensor measurements, header features) can be incorporated as input vectors for the training phase. In preprocessing phase, data in Numeric form converted to nominal form. Accordingly, 5 classifiers are defined for each gateway device with their best estimators.

5.2. Model Creation and Selection

Since this is a classification problem, we must first gather data for both classes (normal and abnormal) and then train the model using Machine Learning methods based on this data using linear or non-linear data. The data can then be categorized using this model. Since classification is more precise than unsupervised models, we apply it. We create a distinct classifier model for each device that serves as the device profile for this reason. We use the binary-class classifier known as One-Vs-Rest, sometimes known as One-Vs-All, which trains one classifier per class.
In order to learn or load the classifier whether it is in the training or testing phase, the ML algorithm will acquire the models for each device after they have been constructed.

5.3. Feature Extraction

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

The real-time sensor data and their header packet information are gathered on the virtual machine and saved in various datasets including header-DB and sensor-DB in this study while taking sensor data and IoT gateways data into consideration. The chosen features must be taken into account during the continuous identity verification process. When the server receives the sensor data, it compares them to the historical values stored in the feature

6. Evaluation

In this section, initially, the testing scenario and performance metrics will be defined. Then, according to the introduced metrics, the classification results will be analyzed in various classification algorithms.

6.1 Scenario Description To evaluate our approach, a prototype system has been established as shown in figure 1. It generally contains six sensors, six IOT gateways, six wireless routers, and a virtual server. In such a prototype, two temperature, humidity sensors, Rainfall sensors and N,P, K sensors are connected to two IOT gateways. By connecting to the Internet through various wireless routers, IOT gateways forward the sensors data in tree based ontology to the server. A wrapper is assumed to running over the IOT gateway which reads the sensor value, translates it to the HTTP POST request. The server assumes to manage the device identification via running the security service. A fake dataset is created randomly to represent the cyber-attack and it is added to the real-time dataset of the smart agriculture.

6.2 Performance Metrics

We used WEKA tool to evaluate the various Machine Learning(ML) algorithms and identify the suitable ML algorithm to detect the Cyber attack. Various performance metrics have been used for the evaluation of the efficiency of the proposed system, which are described below.During the training phase, data are collected for in Comma-separated values(CSV) format in which columns represent the nominated features and each row includes a list of features related to one arriving packet containing sensor data and device identity. The data set is preprocessed for converting Numeric to Nominal data set.

Conclusion

A Smart agriculture will provide better yield simultaneously there is threat by Cyber attacker to forge the data and make system to damage. After proposing this framework and discussion, we learned that this framework using ML algorithm is flexible enough to run on more variety of Dataset. We have performed the analysis using few set of ML algorithm. The important ML algorithm considered: Trees.J48, Bayes. NavieBayes, Lazy.IBK, Functions. Logistic and Trees. Random Forest represents best and worst case results. Our results show a significance accuracy improvement in the measurement-based models. With comparative analysis report we identify that Trees.J48 better result for classification to detect Anomaly. Future work ought to be dedicated to include the number of instances taken at different interval of time. So that attack can be detected in earliest stage to prevent the loss to the system.

Acknowledgement: This research was funded by the Centre of Excellence in Cyber Security (CySek) under Research Development Programme, Karnataka State Council for Science and Technology Bangalore. Grant Number: KSCST/COE-CS/365 Dated 27th SEP 2022. Moreover, Authors would like to acknowledge the CYSEK

for supporting this work that will be applied in smart Agriculture. Further, it was supported in part by the Department of Computer science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India.

References:

1. C. Marwa, S. B. Othman and H. Sakli, "IoT Based Low-cost Weather Station and Monitoring System for Smart Agriculture," 2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Monastir, Tunisia, 2020, pp. 349-354, doi: 10.1109/STA50679.2020.9329292.
2. S. O. Oruma, S. Misra and L. Fernandez-Sanz, "Agriculture 4.0: An Implementation Framework for Food Security Attainment in Nigeria's Post-Covid-19 Era," in IEEE Access, vol. 9, pp. 83592-83627, 2021, doi: 10.1109/ACCESS.2021.3086453.
3. Shah, Trusit and SubbarayanVenkatesan. "Authentication of IoT Device and IoT Server Using Secure Vaults." *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (2018): 819-824.
4. A. N. Jahromi, H. Karimipour, A. Dehghantanha and K. -K. R. Choo, "Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems," in IEEE Internet of Things Journal, vol. 8, no. 17, pp. 13712-13722, 1 Sept.1, 2021, doi: 10.1109/JIOT.2021.3067667.
5. F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021, doi: 10.1109/ACCESS.2021.3131014.
6. M. M. Rana and R. Bo, "IoT-Based Improved Human Motion Estimations Method Under Cyber Attacks," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10934-10935, Dec. 2019, doi: 10.1109/JIOT.2019.2932980.
7. M. Elsisi, M. -Q. Tran, K. Mahmoud, D. -E. A. Mansour, M. Lehtonen and M. M. F. Darwish, "Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning," in IEEE Access, vol. 9, pp. 78415-78427, 2021, doi: 10.1109/ACCESS.2021.3083499.
8. F. Li, Y. Shi, A. Shinde, J. Ye and W. Song, "Enhanced Cyber-Physical Security in Internet of Things Through Energy Auditing," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5224-5231, June 2019, doi: 10.1109/JIOT.2019.2899492.
9. F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, April 2020, doi: 10.1109/TII.2019.2956474.
10. MahdisSaharkhizan, Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo, Reza M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic" IEEE INTERNET OF THINGS JOURNAL, 2020