



ORIGINAL ARTICLE

A CYBER SECURITY MODEL FOR IOT DEVICES FOR THE MANUFACTURING SECTOR

¹*Priyanka Devi Ramesh, ²Dr.T.P. Latchoumi, ³Dr. MVS Prasad

¹ Business Intelligence Engineer, Amazon Virginia, United States

² Associate Professor, Department of Computer science and Engineering, Sri Manakula Vinayagar College of Engineering and Technology, Pondicherry, India

³ Professor, Department of CSE (Data Science), Malla Reddy Engineering college, Secunderabad, India.

Corresponding Author Email: priyankadevi.r1@gmail.com

(Received 08 January 2025; revised 02 March 2025; accepted 02 May 2025)

Abstract

During research and innovation of an Internet of Things (IoT) oriented Networked Embedded System for Industrial Computing Analysis. The purpose of this paper is to provide such an approach to contextual intelligence for the industry. And it focuses on the analysis of big data in the workplace and the creation of a cyber-physical platform with the combination of various current and customized business intelligence solutions based on their operational requirements. This enables parts to be changed and programmed. To tackle industrial computing involving geolocation, sensory and unstructured information for exploring big data, the study develops a carefully planned new context. The proposed networked embedded system concept was demonstrated through a study case. To achieve the next fundamental industrial change, more research into system development and therefore the transition from current manufacturing to industrial automation needs to be done.

Keywords: *IoT; Cyber Physical System; Data Analytics; Context Intelligence*

1. Introduction

To improve operational behavior and activities, integrated industrial socio-technical models and frameworks 4.0 and SPC. To enable particular skills and capabilities, small and medium-sized businesses have integrated new IoT technologies, AI, and program management solutions. Technological breakthroughs were made possible by the clusters of embedded devices, which allowed many workstation components to be processed by computer processes. The system was designed to be smart manufacture because of the computerized numerous tasks, including reconfiguration tricksters, their movements, management, & optimization of robotic systems in a motion planning group schedule [1-2]. To regulate the conversion from obsolete technologies to CPPS, the reference architecture for Industry 4.0 has been proposed. The adaptation solution was validated using an experimental industrial robot arm installation. The development of the intelligent business has just been greatly aided by cutting-edge technology, including big data analytics, industrial 4.0, the IoT, cloud services, and machine intelligence. New industry developments have paved the way for the methodical development of big data, CPS, including Industrial Revolution 4.0 views, which have been thoroughly explored on the manufacturing line [3]. For complex production processes, the necessary studies and calculations have been carried out and therefore the planning of the flooring shop using state-of-the-art CPS technologies has been established. All sectors, including manufacturing, automotive, healthcare, mobility, communications, transport, entertainment, and technology, can benefit from Industry 4.0. The Industrial Revolution 4.0 focuses on information exchange across the entire industry supply chain, as it is a cloud-based computing innovation [4-5]. Due to its experience and understanding, high-tech strategy, and reduced manufacturing complexity, it accelerates an industry in terms of manufacturing facility procedures. Cyber-physical systems were hardware-based, leveraging the Internet as an important network. Cyber-physical technologies have also been used to make things better, simpler, faster, and more efficient in all

industries, including architecture, medicine, transport, and industry [6].

The rapid adoption of Internet of Things (IoT) technologies in the manufacturing sector has transformed existing factories into intelligent, interconnected smart manufacturing environments. Industrial IoT (IIoT) devices such as sensors, actuators, programmable logic controllers, and robotic systems enable real-time monitoring, predictive maintenance, and autonomous decision-making, thereby improving productivity, quality, and operational efficiency. However, the large-scale deployment of heterogeneous and resource-constrained IoT devices, combined with continuous data exchange across shop floors, edge gateways, and cloud platforms, significantly expands the cyber-attack surface of modern manufacturing systems [7]. Cybersecurity has consequently emerged as a critical concern for IoT-enabled manufacturing, where cyber incidents can directly disrupt physical processes, compromise worker safety, and cause severe financial and reputational losses [8]. Unlike conventional IT systems, manufacturing IoT environments integrate cyber and physical components, making them vulnerable to sophisticated attacks such as device spoofing, ransomware, false data injection, denial-of-service, and insider threats. The strict real-time constraints, legacy industrial protocols, and long device lifecycles further complicate the implementation of conventional security mechanisms, rendering many existing IT-centric security solutions inadequate for smart manufacturing contexts [9]. Recent research efforts have explored encryption, authentication, intrusion detection, and access control techniques to secure Industrial IoT systems. Nevertheless, most existing approaches focus on isolated layers or specific attack types, lacking a holistic and scalable security architecture that spans devices, networks, edge intelligence, and cloud-based manufacturing applications. Moreover, the growing reliance on data-driven analytics and autonomous control highlights the need for adaptive, intelligence-enabled security models capable of detecting evolving threats while maintaining low latency and minimal computational overhead [10]. To address these challenges, this work introduces a comprehensive cybersecurity model tailored for IoT-enabled manufacturing systems. The proposed model adopts a layered defense-in-depth strategy that integrates lightweight cryptographic mechanisms, secure communication, edge-level intelligent intrusion detection, and centralized governance and policy enforcement [11]. By aligning cybersecurity measures with the unique operational and real-time requirements of smart manufacturing environments, the model aims to enhance system resilience, ensure data integrity and confidentiality, and support secure and reliable Industry 4.0 operations [12].

2. Related Works

The information volume has ceased to be an unorganized information, but rather a tedious decision to execute since the conventional computer modeling has been enhanced to analyze bulk data. The introduction of a smart factory was actually proposed to execute in industry works such as obscuring, connecting and monitoring the lower and higher synchronized control terminals in advanced production line planning. This has generated new classification, distribution, and coordination among smart devices with adaptability, advanced workstations, content, technology, goods and component manufacture. The systematic 5C framework would come in handy with the development of industrial business intelligence [13]. It incorporates CPS in the manufacturing firm in order to develop interactive devices and smart working areas. Various information acquisition paradigms have been proposed as far as an electronic fusion of production processes. This provides an intelligent production mechanism that enables numerous work places, and optimization of planning to prevent any delays in measurements as well as the structure of the corresponding technologies [14]. The perspectives of research on the characteristics, and functions, including properties of the next project implementation, as well as the associated equipment, had been diverse when considering the calculation of the automation and control system. The most recent structure of an open loop that integrates both moment and event-based systems would assist in accommodating a dynamic world [15-16]. The Internet reload could be simplified with the new asset virtualization routing scheme with the virtualization of the devices that are already on-board. The local real structure that is international and digital may exist. The Networked Embedded System 5Cs Design was also introduced [17]. It has not been studied much to introduce pattern recognition to the existing cyber-physical network as big data analytics, although scientists had established some of the basic ideas regarding such systems. To propose the organization of an environmental intelligence system to study big data seems the aim of the program. The results of the research are not only an occasion to exchange and

analyze the vast volumes of information with the help of further technology. Cloud Technology, Wireless Sensor Networks (WSN), and even IoT generate structured large data sets and correlation with the help of a scientific research approach and further disseminate the brand-new information with scholars and companies [18]. Over the past few years, a number of studies have reported the urgency of having sophisticated security systems in manufacturing set-ups that are specific to the Industrial IoT (IIoT). A general reference on how to adopt and implement secure and privacy-guaranteed IIoT in smart manufacturing summarizes the recent progress in matching operational effectiveness with cybersecurity problems in heterogeneous IT/OT environments [19]. It underlines the effects on integrating IoT devices, which increase real-time processing and automated process flows, but also pose high vulnerability that must be mitigated by maintaining strong privacy protection and secure communication systems to facilitate the robust production systems. Thematic literature reviews based on the architectural and defense concepts have explored ways of securing Industry 4.0 with the artificial intelligence method and provenance blockchain technology as means of fortification in cloud manufacturing [20]. These surveys talk about how artificial intelligence can be used to improve anomaly detection and response systems in IoT systems, and provenance blockchain can be used to provide traceability and resistance to tampering, solving the data integrity issues related to the connected factories. These publications demonstrate the value of using a combination of different emerging technologies to strengthen the IoT infrastructure against advanced attacks that are aimed at connected manufacturing resources. The second area of research is privacy-saving intrusion detection systems based on decentralized learning systems that are applicable in IIoT [21]. The most recent work suggests a Federated Learning-Enhanced Framework of Blockchain which integrates federated learning to obtain collaborative detection with blockchain smart contracts to ensure safe model updates and anomaly records in edge devices. The experimental findings showed a better detection rate and communication efficiency in relation to centralized IDS approaches, which is promising with regard to scalable, privacy-conscious threat detection with respect to industrial applications. Besides applied frameworks, researchers have also come up with conceptual models, which analytically examine cyber-physical vulnerabilities peculiar to smart manufacturing. An attack vulnerability identification and classification taxonomy with a defense-in-depth orientation defines the existing security solutions as requiring expansion to consider manufacturing-specific attack vectors in the form of process monitoring lapses and human errors. Such taxonomy does not only help in vulnerability assessment but also helps in designing of the defense mechanisms that will be layered in order to protect the critical assets of industrial setups in an effective way.

3. PROPOSED METHOD

Based on a novel information and communication documented information, stack designed architecture and even multiple algorithms to predict, trend excavation and recognition, as well as energetic organization creation and upgrading, a situational platform to manufacture information systems analytics would be created in this research. The proposed system is supposed to assist different companies in cultivating their capability to capitalize on the environmental awareness movement. Requesting companies do not need to be concerned with development of expensive and complex big data analytics systems with a false return on investment any longer. The study offers a significant connection between them and the assimilation of various engineering technology techniques and large data analytics, which would dispose of these IE techniques to transform to generate more significant and advanced results. The proposed product subscription alternatives could assist companies not only to save significant amounts of money on staff, but also to gain considerable knowledge about consumer behavior, and certain market trends, including technological progress. The companies could apply this knowledge to their benefit by updating their business strategy, developing new opportunities, and ensuring the rapid responsiveness to the solution of the problems. When the integrated platforms are successfully developed, this must continuously generate new patterns and correlations which relate to various occurrences and remain with the information cycle in the field of mining engineering and certain other areas of study. It is designed and built in a stack-based design which would integrate many well-established, yet rather trade secrets analytics processes, a new platform of inter-process communication to provide data to many interconnected phones, and it is an introduction intellectual ability automated system that would have to deal with manufacturing informatics regulations, the study can make a major

contribution to the innovative managed service of manufacturing information systems analytics. The results of the study would lead to new research directions through continuous dissemination of the new knowledge and trail the path to an all-encompassing approach to address the issues of industrial designs as experienced in the sectors. Figure 1 illustrates that context engineering, security in big data analytics has 5 levels, a session layer, an analytic surface, a data tier, a core network and an IoT overlay. All the details of gradient descent are presented in sections B, C, D, E, and F, respectively.

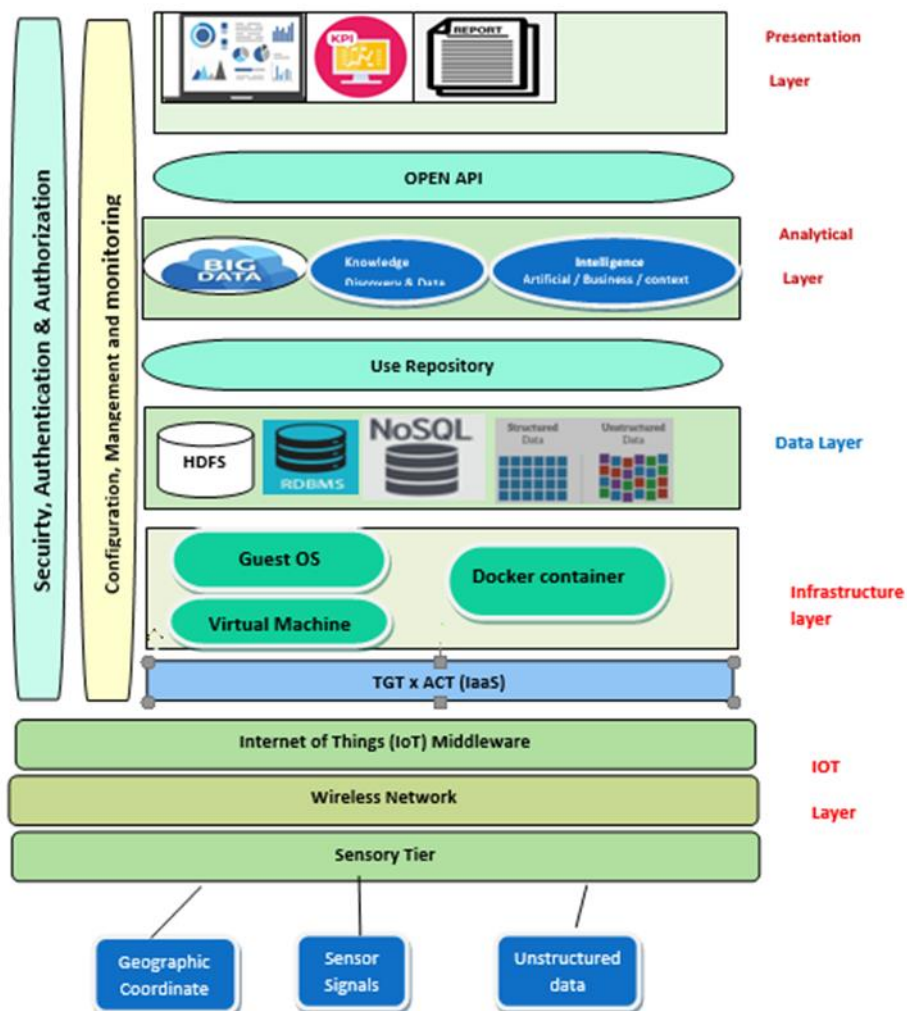


Figure 1: Context Intelligence Architecture

The system would present the identified trends to domain experts in the form of a dashboard, key performance metrics or report through the session layer. Visual fact gathering can enable production planning to know the actual performance of any of the workstations, equipment or even employees. Since sensors and Internet of things devices can gather both information equipment as well as the development process, the dashboards also have a discrepancy between the desired and alternative measurement of the items that are manufactured by various machines to manufacturing units. The analysis procedure involved the use of an aggregation algorithm to assist information groups accessing meaningful information or models. Unsupervised learning set was compiled to bring out the models or models available. The existing cluster is to find out the intrinsic classification in a set of unlabeled information. An example is the agglomeration nesting that appears to be an old form of clustering that employs the fuzzy clustering method. AGNES The first step is to allocate one item of data to one group via a bottom-up technique. This was followed by the selection of groups that are the most similar. The natural information clusters would be identified through the method of determining the dissimilarity between two groups based on the solitary connection, the process of assembly, and the medium of interconnection. Moreover, project identification data were unclear, erroneous, and incomplete in the real conditions. Fuzzy

clustering has been found to give human motion correlations. Fuzzy clustering was used to take sample profiles during the survey. It has the ability to form overlapping groups. Various levels of participation may be assigned to the knowledge bases in more than one cluster. Sample profiles in the survey were sampled using a fuzzy cluster that is able to generate overlapping sample groups. This work also incorporated the fuzzy c-means algorithm and also its steps were illustrated below.

(S1) Fix c, m, A $||k||A$ Choose an initial matrix $Y(0) \in M_k$. Then at step $k, k = 0, 1, \dots, LMAX$.

(S2) Compute means $v^{((k))}, x = 1, 2, \dots, c$ with equation (1).

(S3) Compute an updated membership matrix $u^{((k+1))} = u_{xk}^{((k+1))}$ with equation 2.

(S4) Compute $u^{((k+1))}$ to $u^{((k))}$ in any convent matrix norm, If $||u^{((k+1))} - u^{((k))}||$ with equation 2.

$$u_x = \sum_{k=1}^N (u_{xk})^m j_k / \sum_{k=1}^N (u_{xk})^m, 1 \leq x \leq c \quad (1)$$

$$u_{xk} = (\sum_{y=1}^c (d_{xk}/d_{yk})^{2/(m-1)})^{(-1)}, 1 \leq k \leq N; 1 \leq x \leq c \quad (2)$$

The information was at the data level and managed and stored through Docker containers and cloud computing of the infrastructural layer of the system. It would be proposed that Figure 2 presented in Appendix under the name of the new standardized communications protocol would be used to share and interact information. The company today has the potential to obtain large volumes of information through sensors or communication system providers, as well as structural information through ERP and CRM relational database systems. A NoSQL database and even the distributed filesystem HDFS Hadoop, when combined, permit a large automatic failover and process big data, which have been utilized to store big data. HDFS is universal in hardware and software components, therefore, cyber-physical technologies may be applied to different manufacturing purposes. The proposed standard approach, which encompasses physical connections, conditions of the information, and communication content, could create a reliable method and environment of information interaction and exchange between a great number of sensors and related devices.

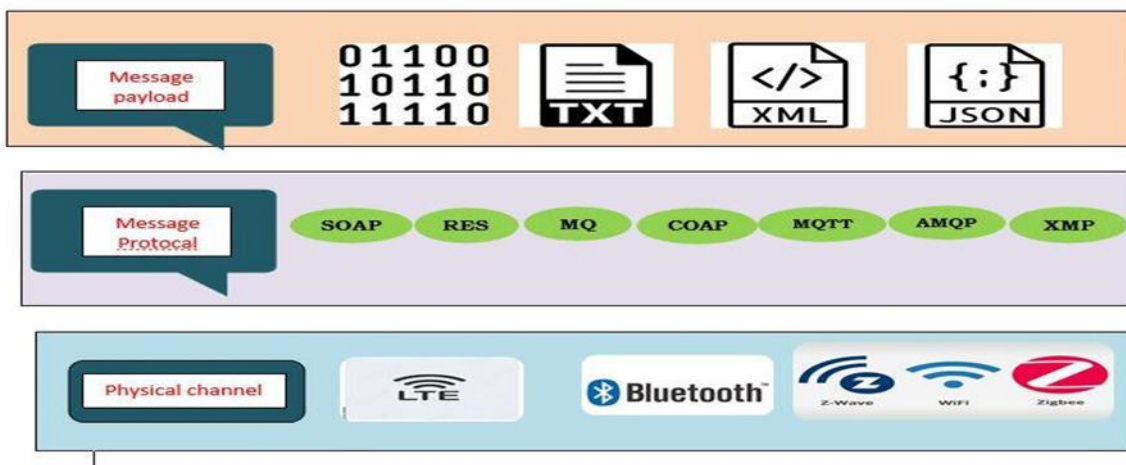


Figure 2: Architecture of Communication and Data Exchange Protocol

The engineers in the construction industry might find it easier to take the information presently held by businesses and transfer it to the system through the use of statistical tools or methods within the operation layer, and thereafter perform big data analysis through the use of the system development and integration. The platform as a service enables the infrastructure improvement cost to be availed by the modern business in another manner with the flexibility scale. Companies could use IaaS to implement the newest applications in automating and monitoring networks. The feature could be done in a software

application or docker container to do an unplanned or experimental workload. IoT layers receive the information of the IoT systems, and this information may be the location or sensor outputs among other unstructured systems. The production may have sensors that would check the temperature and the light output. It was found that an analysis of the workplace that is too bright may be harmful to productivity. It is possible to increase the production capacity with the help of the instruments to monitor the intensity of the light in a workspace where there are more devices connected to a network of sensors to identify different desktops. Provided that the applications were imaginable by itself, the IoT might provide even further radical technology.

3.1 Dataset description

The data that will be used in this study is set to reflect the realistic cybersecurity conditions in a smart manufacturing environment based on IoT and demonstrated in Table 1. It comprises the information gathered by heterogeneous situational Industrial IoT (IIoT) devices utilized on various levels of a manufacturing system, sensors, actuators, programmable logic controllers (PLCs), and edge gateways. The dataset is an example of both normal operation behavior and malicious operations which represent real-life manufacturing processes including monitoring machine condition, controlling production lines, and predictive maintenance. The sample data contains network traffic flows, device telemetry, and control commands, system logs collected in different load and operating conditions.

A single record of data includes all the features (network-level variables (packet size, protocol type, rate of transmission, latency), device-level variables (CPU usage, memory consumption, firmware status), and process-level variables (sensor readings, actuator states, timing constraints). The data is classified into various categories that usually comprise of the normal behavior and common types of attacks that include denial-of-service (DoS), spoofing, false data injection, replay attacks, and unwarranted access. The dataset is preprocessed to provide strong robustness and generalization, which is why it is appropriate to use it in training and testing machine learning and deep learning-based intrusion detection and cybersecurity models of manufacturing IoT systems.

Attribute	Description
Domain	IoT-enabled Smart Manufacturing (Industry 4.0)
Data Source	IIoT sensors, PLCs, edge gateways, network traffic
Data Type	Network traffic + device and process telemetry
Classes	Normal, DoS, Spoofing, False Data Injection
Feature Types	Network, device resource, process-level features
Labeling	Supervised, multi-class
Preprocessing	Normalization, noise removal, class balancing
Dataset Split	Train–Validation–Test
Purpose	Intrusion detection and attack classification
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score

Table 1: Dataset Description

Record ID	Device Type	Protocol	Packet Size (Bytes)	CPU Usage (%)	Latency (ms)	Sensor Value	Attack Type
1	Temperature Sensor	MQTT	512	18.5	12	68.2	Normal
2	PLC Controller	Modbus/TCP	1024	42.3	28	1.00	DoS
3	Pressure Sensor	CoAP	256	15.1	10	3.45	Normal
4	Robotic Arm	OPC-UA	768	55.6	35	0.87	Spoofing
5	Edge Gateway	HTTP	1500	68.9	50	0.00	False Data Injection

Table 2: Sample data

The sample data is a representation of communication and operational logs of IoT-enabled manufacturing devices, which captures network behavior, resource utilization by the device, and sensor measurement presented in Table 2. Normal and attack cases like DoS, spoofing, and false data injection are marked to facilitate supervised learning to achieve effective intrusion detection in a smart manufacturing system.

3.2 Data Pre-processing

The raw manufacturing IoT data is preprocessed systematically in order to enhance detection accuracy and stability of the model. Mean imputation is used to address the missing values: $x_i = \{x_i, \text{if } x_i \text{ exists } \frac{1}{N} \sum_{j=1}^N x_j \text{ otherwise} \}$ (3)

Feature normalization is applied using Min–Max scaling to ensure uniform feature ranges:

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (4)$$

To address class imbalance, data resampling is performed so that each class has approximately equal samples:

$$N_c \approx N_k \forall c, k$$

Finally, the preprocessed dataset is divided into training, validation, and testing sets to support robust and unbiased model evaluation.

4. Case Study

The economy in India has developed at a rapid rate, and pollution is the first unwanted effect. In the case of the neighborhood, one-stop environmental providers are not that many. The activity in this study case seems to be one of the environmental telecommunications operators in the clean-up industry. The industrial washing solution entails diverse environmentally friendly, hygienic, washing, and disinfection processes. Has found it difficult to determine the position of the current status in the traditional dishwasher plant regarding the decision to accept or not to accept the new ad hoc request due to the possibility of lack of comprehensive and presentation to the user. Also, one would not find it easy to track and trace goods like boxes, baskets, and dollies. The client firm senior managers knew the importance of openness in information and physical planning control. They are interested in establishing a cyber-physical model that appears to be an IoT as a consequence. In order to do survey work and site assessment, which involves pilot deployment, collaborative research between academics and industry was created. The network providers and manufacturers are now in a position to employ the IoT cyber-physical processes with the assistance of this study. Introduction awareness algorithm was used and evaluation experience was conducted by incorporating traditional algorithms of big data analysis, information extraction and information extraction to the proposed system. Geographic data, senses, and a great deal of other unstructured data is first collected. Second, the fuzzy set theory would transform statistical data into discrete data. The Environmental Awareness Program would be able to use discreet information and review it to give useful trends. The researchers in the service sector may directly comprehend the identified compliance with customer requirements of the proposed framework, and may provide new advertisement or actionable knowledge to enhance their production process to meet customer demands as a company.

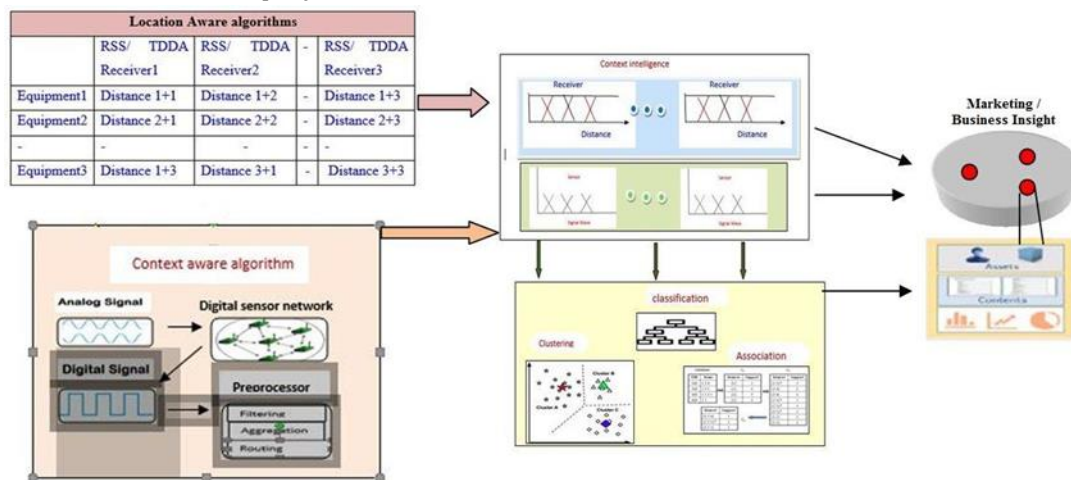


Figure 3: Context Intelligence working

The organizational context may have several needs of the dish cleaning service to the individual consumers, such as the pick-up and delivery times of the dishes, number of dishes and the type of dishes.

This could lead to numerous service conditions and agreements. There are several service needs which enable similarities in client groups to be classified. This was followed by an assigned level of compliance to all the operational needs. Depending on the quality of service provided as indicated, various segments of clients are combined utilizing the fuzzy c-means segmentation. As an example, a student will be able to request the washing and transportation of ten hours of 15 containers of plates and 8 containers of utensils. The number of clusters can be used to define a customer order by designers in three phrases. The number of containers of food and tableware used was few, moderate, and numerous, but short, intermediate and long might be applied to the duration it takes to wash dishes from the time they were picked up to the time they were delivered. This renders the inability to clearly define grammar property in terms of center among the values of these samples and each character could be assigned an adhesion function. The values above were centered on as axis values of probability distribution belonging values. An IoT-based cyber-physical world is a multi-level decentralized cloud environment that contains hierarchically structured global and regional parts. Although a global network has been utilized to enhance the network performance to help appropriate circulation of automobiles between various plants, a local approach has been employed in providing reduced latencies that would provide effective local dishwashing operations. The data gathered by RFID both in the establishment and through digital displays has been presented in Figure 4. The different initial points of operations may be viewed in Figure 4, the flow of the dishes in and out, as well as the informational processing of the maintenance of the stock between the cart and the container. Besides involving the use of technology devices within the government regions, the global process involves the assignment of tasks and delivery notes through communication devices which can be observed in Figure 5.

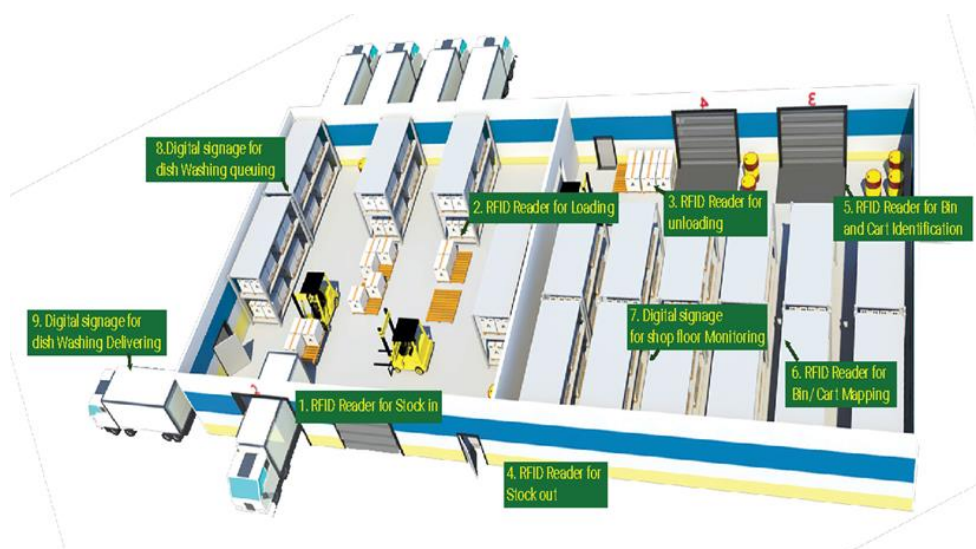


Figure 4: RFID deployment

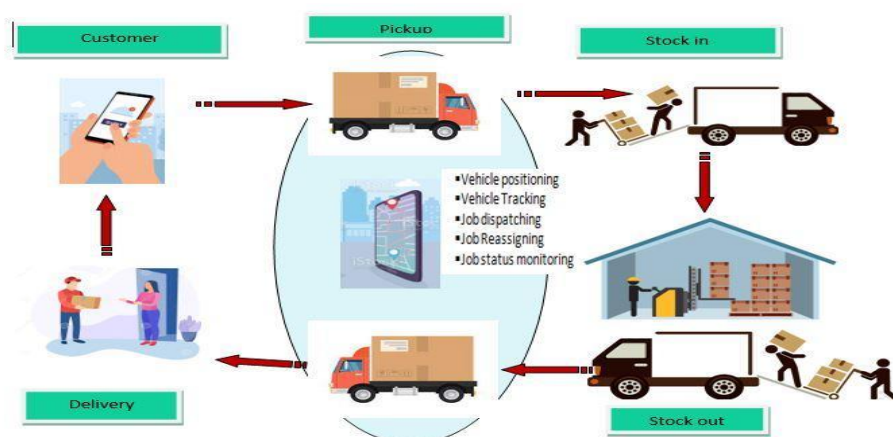


Figure 5: Fleet administration

The multi-level decentralized cloud service allows the reliable distribution and information management of vehicle and dishwasher activities. The proper fleet management might be achieved with the implementation of the IoT-based pervasive computing that would enable the right truck to be deployed to pick up the dirty dish and deliver the cleansed dishes to the restaurants within the required timeframe with the minimum carbon footprint. Being an ecological service provider, consume low-cost resources such as dishwashing machines, fresh water, energy and washing solutions in dishwashing activities. The amount of frequency by which these resources are used can be measured by the IoT-based system. The firm may use recycled water, as well as a deep learning of wasted food to decrease the amount of waste. Therefore, it promotes environmental and economic efficiency.

Algorithm

Input: Raw IoT data $D=\{x_1, x_2, \dots, x_N\}$, from sensors, PLCs, and gateways

Output: Attack classification label $y \in \{\text{Normal, DoS, Spoofing, FDI}\}$

Step 1: Data Acquisition

Collect real-time data streams from manufacturing IoT devices: $x_i = [f_1, f_2, \dots, f_m]$ (5)

where f_m represents network, device, and process features.

Step 2: Pre-processing

Normalize features using Min–Max normalization: $x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}}$ (6)

Step 3: Feature Extraction

Extract discriminative feature vector: $F = \phi(x_i^{norm})$ (7)

Where $\phi(\cdot)$ denotes feature mapping.

Step 4: Intrusion Detection Model

Compute anomaly score using a learning model (e.g., deep classifier): $z = WF + b$ (8)

Apply SoftMax for multi-class attack probability: $P(x_i) = \frac{e^{z_k}}{\sum_{j=1}^K e^{z_j}}$ (9)

Step 5: Decision Rule

Classify the instance as: $\hat{y} = \arg \max_k P(y = k | x_i)$ (10)

Step 6: Response and Mitigation

If $\hat{y} \neq \text{Normal}$, trigger mitigation:

Action = {Isolate device $\hat{y} = \text{DoS}$ Reauthenticate $\hat{y} = \text{Spoofing}$ Discard data $\hat{y} = \text{FDI}$ } (11)

Step 7: Model Update

Update parameters using cross-entropy loss: $L = \sum_{k=1}^K y_k \log \log (P(x_i))$ (12)

The suggested cybersecurity algorithm constantly tracks the information provided by the IoT devices on the manufacturing floor such as the network traffic, device resource consumption, and process-level parameters. The data are collected and preprocessed first to eliminate the noise and differences in scales to have a stable learning behavior. The corresponding security features are then mined and used into an intelligent intrusion detection model to calculate the likelihood of each case being a normal or an attack case. According to the maximum probability decision rule, the system categorizes the detected activity and initiates the relevant mitigation measures including the isolation of the device, re-authentication, or data rejection. Loss minimization is used to periodically update the model to fit the changes in cyber threats and retain the real-time efficiency of the operations in smart manufacturing systems.

5. Results and Discussions

The test facility will be created to assess the efficiency of the offered cybersecurity system in an IoT-based smart production facility. The tests will be run on a simulated manufacturing testbed including heterogeneous IoT devices including sensors, PLCs, robotic units and edge gateways that use industrial communication protocols. The processed data is separated into training, validation and testing sets so that the data is not biased in assessment. The model of intrusion detection is trained on the basis of supervised learning with optimized hyperparameters, and the performance of the model is evaluated by the accuracy, precision, recall, F1-score, and detection latency. Every experiment is carried out repeatedly in order to achieve the consistency and reliability of the achieved results in various scenarios of attack.

Hyperparameter	Value	Description
Learning Rate (η)	0.001	Controls weight update magnitude
Optimizer	Adam	Adaptive gradient optimization
Batch Size	64	Number of samples per training iteration
Number of Epochs	50	Total training iterations
Hidden Layers	2	Depth of the intrusion detection model
Neurons per Layer	128	Model capacity
Activation Function	ReLU	Non-linear feature learning
Output Activation	Softmax	Multi-class classification
Loss Function	Categorical Cross-Entropy	Classification error minimization
Regularization	Dropout (0.5)	Prevents overfitting
Train-Test Split	70:30	Dataset partitioning

Table 3: Hyperparameter settings

The hyper parameters are chosen in order to balance detection and computation efficiency to the manufacturing conditions of the IoT shown in Table 3. A low learning rate will produce stable and rapid convergence of the Adam optimizer, whereas a moderate batch size will enhance generalization. Through the usage of multiple hidden layers filled with ReLU activation, it is possible to learn features effectively, and softmax allows the classification of multi-class attacks. The regularization of dropout minimizes overfitting which makes it dependable in detecting intrusion in varied conditions of manufacturing attacks.

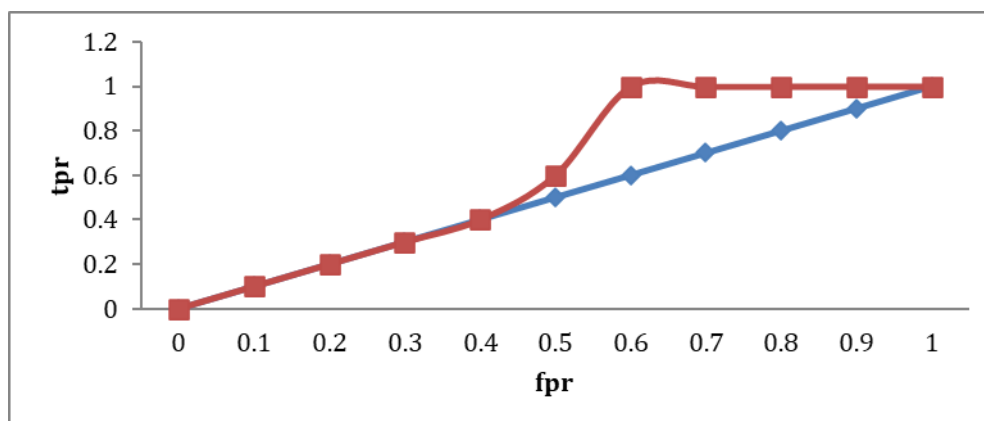


Figure 6: RF's evaluation criteria

NB appears to be a segmentation technique, which makes powerful assumptions about the independence of the covariates in the application of the Bayes rule presented in Figure 6. The classifier incorporates a Gaussian distribution of numerical predictor variables whose mean and median are computed out of the training stage in order to differentiate between normal and malicious information. It assumes liberty between the covariate's characteristic limited on the relationship with the services and a normal distribution of the regression coefficient characteristics. The Laplace flattening algorithm was used to predict the probability of the malicious and benign subclasses. The characteristics of the NB have been changed using such variables. Figure 5 showed the confusion matrix and performance metrics of the Naive Bayes model of using the Training and test set of the ton-IOT net dataset. This approach does not

work well as compared with the GBM and RF approaches depicted in Figure 7

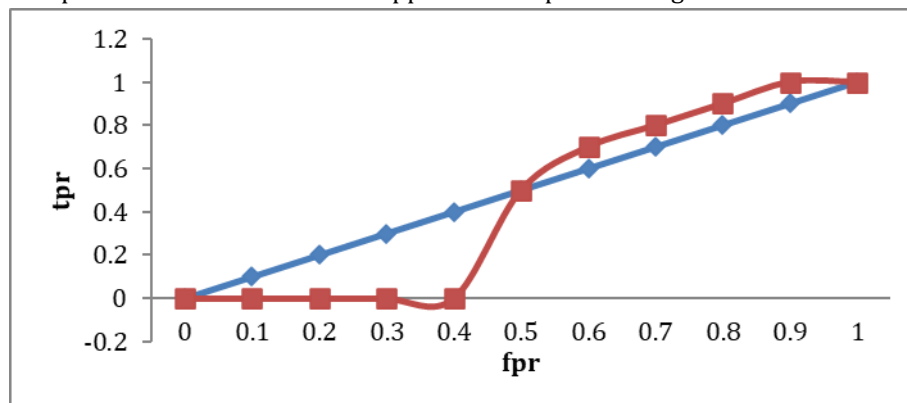


Figure 7: NB's evaluation criteria

DNN appears to be a multi-layered convolutional artificial classic method through learning algorithm and stochastic gradient. The connection has been altered to detect normal and malicious information by the addition of fifteen hidden nodes that consist of fifteen layers with one of the tan-h activation parts, ten cross-validation epochs, and a SoftMax activation within the production tiers component. The metrics of evaluation and confusions matrix of such a Prediction model on the Training and test subset of the Ton-IOT dataset in figure 6 demonstrates that RF was weak and the other two methods were stronger in training and test data, which is a small portion of a complete dataset, enabling the 4 supervised learning methods to perform. Characteristics generated under this database demonstrate a significant difference in variances between normal activities and malicious activities, hence the results were realized.

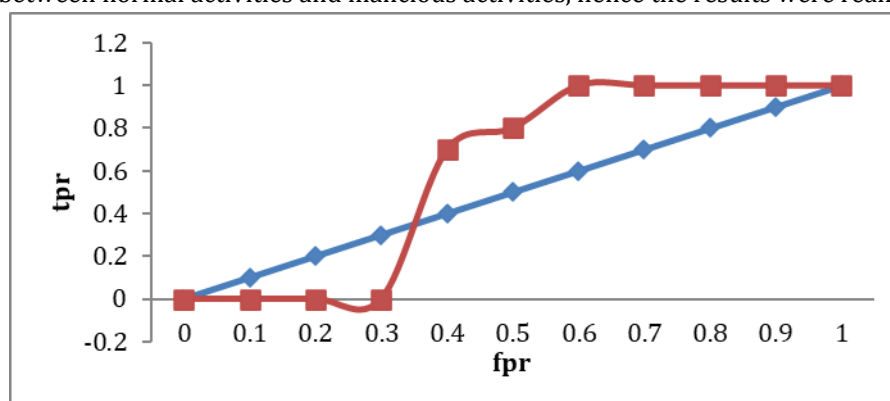


Figure 8: DNN's evaluation criteria

Test and train the algorithms with a small percentage, and we are using the IP addresses as well as ports that aid in distinguishing between normal and malicious observation, hence the results of the structures are quite good in terms of prediction performance and false-positive rate. To ensure the intricacies of the threat and real practices related to the dataset, we recommend that we eliminate IP addresses and ports when measuring the machine learning-based protection algorithms when employing all the information of the dataset in lieu of what is depicted in Figure 8.

Table 4 indicates the major disparities between the two data - sets to possess a valid evaluation in this case between the Ton-IOT data and the quite well versions. KDD-99 and NSLK-DD databases were outdated and a representation of current traffic in the network is barely not displayed in the table. CAIDA and UNIBS datasets traffic flow and architecture existed in reality, but neither of the data utilizes multiple sources of data as well as would label it with such a small percentage of intrusion incidents. The DEFCON and LBNL data lacks differentiated datasets since they have been acquired through a network simulator in gathering the diverse assault operations. The TUIDS ISCX and CICDS2017 data were obtained in real-life environments and also possess full data loss protection with a variety of regulatory concerns, thus, comprising of just internet traffic that lacks heterogeneous information. The DARPA-2009 data was

obtained due to a realistic sense though its accuracy cannot be relied on as it is not marked with such a large proportion of packet headers.

Datasets	Realistic network config.	Realistic network traffic	Labeled observations	Heterogeneous data sources	Total interaction capture	Full packet capture	Many malicious scenarios
DARPA-2009	True	True	False	False	False	True	True
UNSW-NB 15	True	True	True	False	True	True	True
N-BaloT	False	True	False	False	False	False	True
BoT-IoT	True	True	True	False	True	False	True
New TON_IoT	True	True	True	True	True	True	True

Table 4: Comparisons of popular datasets

The UNSW-NB-15 has been developed in such an operational environment that merely has internet traffic and various attacker scenarios. This N-BaloT and BoT-IoT data was created with the purpose of collecting botnet activities on internet traffic of IoT applications. The major weakness that incorporates both data pertains to the fact that the telematics data of the Internet of Things functioning does not exist, and could be employed to construct the IoT protective measures. In addition, the Ton-IoT dataset was produced by the use of a new model environment which considers the interaction between the edge, fog and cloud layers. Using common and hostile situations, researchers have revised them with actual ground truth tables which validate the occurrence of hostile strike actions. These allow complete internet traffic recording, and record-keeping of various OS, including the information in the IoT. This makes the Ton-IoT data unlike a great variety of other databases that collect information by various heterogeneous sources such as internet traffic, data in Windows and Linux operating environments and telematics based on the IoT internet services. The 4 sources of information have been identified using the same dates and time of intrusion activities that utilized weak networks. An ensemble learning system that could in fact analyses internet traffic, audit trails of windows OS, involving sensor data may be created to identify abnormal results through the data transmission, OS, and IoT devices, such as sensor information. The dataset actually enhances the properties of four datasets to create new supervised ml security mechanisms. Although the key objective of the existing databases has never been to evaluate detection mechanisms. The internet of things datasets is fine-tuned to determine the effectiveness of different ML-based security measures, i.e., malware-detecting, privacy-protecting, and cyber-threatening, vulnerability-packs, and even computer-forensic functionality. The data might be applied to analyze the possibilities of using security measures of the host machines, IoT infrastructures, internet connections, fog, clouds, edges, and development tools infrastructures. It was a byproduct of the prospective study of the existing test platform technology that involved such technologies and running of both regular and targeting situations.

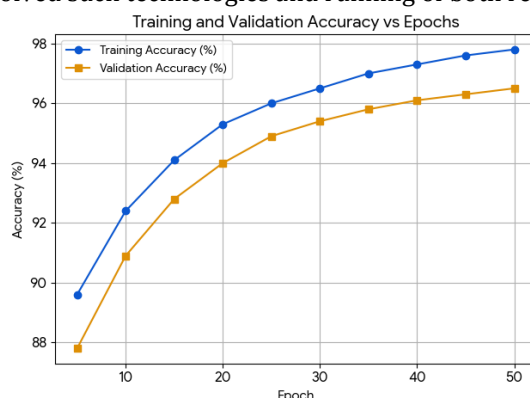


Figure 8: Comparison of training and validation accuracy

Figure 8 demonstrates how the accuracy of the proposed model in terms of training and validation improved with the number of epochs in the process of cybersecurity modeling. First, the two accuracies improve fast as the model acquires the hidden trends in the IoT manufacturing data. This convergence can be seen as the improvement in the training is slow. The model has a high training and validation

accuracy of 97.8 and 96.5 respectively in the last epoch and this indicates that the model generalizes effectively on unseen data and does not overfit, hence it can be used in real-time to detect intrusion in the smart manufacturing environment.

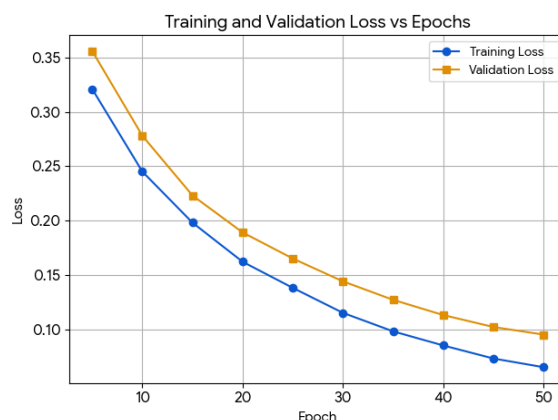


Figure 9: Comparison of training and validation loss

Figure 9 shows that the proposed cybersecurity model decreases the training and validation loss at a rate of 50 epochs. The two losses reduce progressively, which means that the model is learning the trends in the IoT manufacturing data. The training loss is 0.065 and the validation loss is 0.095 by the last epoch and there are great convergence and low overfitting. This shows that the model can well make inferences based on invisible data, hence can be used to enable trusted real-time intrusion detection in intelligent manufacturing settings.

6. Conclusions

In order to obtain progressing productive learning and production on behalf of the entity that it is associated with, an IoT-based pervasive computing system was created with the unique features of data analyses and optimization methods. It is the maximum efficiency of operations. This proposed government was operated particularly through the incorporation of RFID technology which would be identified as a proven technology that may streamline the processes of incoming logistics. The capacity of this proposed IoT-based cyber-physical world to progressively incorporate workflow assessment to facilitate relevant researches on Industry Big Data Analytics was projected to have significant influence at all on the smart track and control of the study.

Conflict of Interest Statement

Not applicable

Data Availability Statement

Data not available due to commercial restrictions

Authors' contributions

A: Writing- Original draft preparation, Visualization, Investigation

B, Supervision, Reviewing and Editing.

Funding

No funding received

References

- [1]. Zhang, K., Cao, J., and Zhang, Y. "Adaptive Digital Twin and Multiagent Deep Reinforcement Learning for Vehicular Edge Computing and Networks." *IEEE Transactions on Industrial Informatics*, vol. 18, no. 2, 2021, pp. 1405-1413. DOI: 10.1109/TII.2021.3054771.
- [2]. Xue, Z., et al. "A Resource-Constrained and Privacy-Preserving Edge-Computing-Enabled Clinical Decision System: A Federated Reinforcement Learning Approach." *IEEE Internet of Things Journal*, vol. 8, no. 11, 2021, pp. 9122-9138. DOI: 10.1109/JIOT.2021.3059637.
- [3]. Vimal, V., et al. "Comparison of Adaptive Filtering Scheme for Sustainable and Efficient

- Communication in Smart City." *Sustainable Energy Technologies and Assessments*, vol. 47, 2021, art. no. 101472. DOI: 10.1016/j.seta.2021.101472.
- [4]. Zhou, S., Jadoon, W., and Shuja, J. "ML-Based Offloading Strategy for Lightweight User Mobile Edge Computing Tasks." *Complexity*, 2021. DOI: 10.1155/2021/7391236.
- [5]. Fu, Y., et al. "Energy-Efficient Offloading and Resource Allocation for Mobile Edge Computing Enabled Mission-Critical Internet-of-Things Systems." *EURASIP Journal on Wireless Communications and Networking*, 2021, no. 1, pp. 1-16. DOI: 10.1186/s13638-020-01828-5.
- [6]. Monica, M., et al. "PMSG-Based WECS: Control Techniques, MPPT Methods, and Control Strategies for Standalone Battery Integrated System." *AIP Conference Proceedings*, vol. 2405, no. 1, AIP Publishing LLC, Apr. 2022, p. 040013. DOI: 10.1063/5.0076438.
- [7]. Yar, H., et al. "Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm." *Sensors*, vol. 21, no. 14, 2021, p. 4932. DOI: 10.3390/s21144932.
- [8]. Minu, M. S., Aroul Canessane, R., and Subashka Ramesh, S. S. "Optimal Squeeze Net with Deep Neural Network-Based Aerial Image Classification Model in Unmanned Aerial Vehicles." *Traitement du Signal*, vol. 39, no. 1, 2022, pp. 275-281. DOI: 10.18280/ts.390127.
- [9]. Pérez, S., Arroba, P., and Moya, J. M. "Energy-Conscious Optimization of Edge Computing through Deep Reinforcement Learning and Two-Phase Immersion Cooling." *Future Generation Computer Systems*, vol. 125, 2021, pp. 891-907. DOI: 10.1016/j.future.2021.07.016.
- [10]. Aazam, M., Zeadally, S., and Flushing, E. F. "Task Offloading in Edge Computing for ML-Based Smart Healthcare." *Computer Networks*, vol. 191, 2021, art. no. 108019. DOI: 10.1016/j.comnet.2021.108019.
- [11]. Teoh, Y. K., Gill, S. S., and Parlikad, A. K. "IoT and Fog Computing-Based Predictive Maintenance Model for Effective Asset Management in Industry 4.0 Using ML." *IEEE Internet of Things Journal*, 2021. DOI: 10.1109/JIOT.2021.3101410.
- [12]. Haseeb, K., et al. "Intelligent and Secure Edge-Enabled Computing Model for Sustainable Cities Using Green Internet of Things." *Sustainable Cities and Society*, vol. 68, 2021, art. no. 102779. DOI: 10.1016/j.scs.2021.102779.
- [13]. Devi, G. N. R., et al. "Development of Medicinal Industries in Building a Replica to the Damaged Human Tissue for Artificial Organs with the Application of Micro-and Nano Technology (MNT)." *Journal of Optoelectronics Laser*, vol. 41, no. 3, 2022, pp. 79-83.
- [14]. Rosero, D. G., Díaz, N. L., and Trujillo, C. L. "Cloud and ML Experiments Were Applied to Energy Management in a Microgrid Cluster." *Applied Energy*, vol. 304, 2021, art. no. 117770. DOI: 10.1016/j.apenergy.2021.117770.
- [15]. Karnan, B., and Kuppusamy, A. "Graph Theory and Matrix Approach for Machinability Enhancement of Cryogenic Treated Cobalt Bonded Tungsten Carbide Inserts." *International Journal of Heat and Technology*, vol. 39, no. 4, 2021, pp. 1372-1382. DOI: 10.18280/ijht.390434.
- [16]. Rathore, S., Park, J. H., and Chang, H. "DL and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT." *IEEE Access*, vol. 9, 2021, pp. 90075-90083. DOI: 10.1109/ACCESS.2021.3089305.
- [17]. Subashka Ramesh, S., et al. "E-Voting is Based on Blockchain Technology." *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, 2019, pp. 107-109. DOI: 10.35940/ijeat.E1021.0585C19.
- [18]. Gasmi, K., et al. "A Survey on Computation Offloading and Service Placement in Fog Computing-Based IoT." *The Journal of Supercomputing*, vol. 78, no. 2, 2022, pp. 1983-2014. DOI: 10.1007/s11227-021-03827-8.
- [19]. Subashka Ramesh, S. S., et al. "Analytics and ML Approach to Generate Insights for Different Sports." *International Journal of Recent Technology and Engineering*, vol. 7, no. 6, 2019, pp. 1612-1617. DOI: 10.35940/ijrte.F8545.038620.
- [20]. Sridharan, K., and Sivakumar, P. "A Systematic Review on Techniques of Feature Selection and Classification for Text Mining." *International Journal of Business Information Systems*, vol. 28, no. 4, 2018, pp. 504-518. DOI: 10.1504/IJBIS.2018.093301.
- [21]. Gill, S. S. "Quantum and Blockchain-Based Serverless Edge Computing: A Vision, Model, New Trends and Future Directions." *Internet Technology Letters*, 2021, e275. doi:10.1002/itl2.275.