9INTRUSION DETECTION SYSTEM FOR CYBER SECURITY IN SMART AGRICULTURE WITH ABCIS TECHNIQUES

NASREEN SULTANA QUADRI, DR. YASMEEN, K DURGA CHARAN, K SURESH BABU, DR. SHAHANA TANVEER, K. SHYAM SUNDER REDDY, DR.M. KIRAN KUMAR

Lecturer, Dept of CSI, College of Science, Zulfi، Majmaah University, KSA.
Assistant Professor, Department of CSE (Data Science), CVR College of Engineering, Hyderabad, India.
Assistant Professor, Narasaraopeta Engineering College (Autonomous), Andhra Pradesh, India.
Assistant Professor at CSE-Data Science, Madanapalle Institute of Technology and Science, Madanapalle, India.
Associate Professor, Department Of CSE, Deccan College of Engineering and Technology, Hyderabad.
Department of CSE, Maturi Venkata Subba Rao (MVSR) Engineering College, Hyderabad
Asst.Prof, Department of CSE, *GITAM* (Deemed to be University), Hyderabad.

ABSTRACT

In this research, we examine and evaluate intrusion detection systems for cyber security in Agriculture 4.0. In particular, we outline the assessment criteria and cyber security risks that are utilised to assess an intrusion detection system's effectiveness for Agriculture 4.0. Then, we assess intrusion detection systems in light of cutting-edge technological developments, such as cloud computing, fog/edge computing, network virtualization, Internet of Things, autonomous tractors, drones, industrial agriculture, and smart grids. We offer a thorough classification of intrusion detection systems in each developing technology, based on the machine learning approach utilised. In addition, we provide public datasets and the frameworks used for implementation that were used to assess intrusion detection systems' performance for Agriculture 4.0. Lastly, we discuss the obstacles and potential lines of inquiry for future studies in intrusion detection for cyber security in Agriculture 4.0. Based on several technical paradigms, a new industrial revolution is underway. "Industry 4.0" (I4.0) is a concise way to communicate the desire to promote and direct this phenomena. Projects falling under this umbrella term are united by the belief that numerous critical technologies supporting Big Data Analytics and Cyber-Physical Systems are merging to form a new, highly automated, distributed, and dynamic production network. To ensure that this process proceeds smoothly and on schedule, new laws and cultural norms must be put in place. In this paper, we exclusively address the technological side, emphasising the exceptional I4.0 complexity that has been documented in the scientific literature.

Keywords: *ABCIS, IoT, blockchain, cyber intrusion detection, cloud computing, AI, SDN.*

1.INTRODUCTUON

The agricultural sector had significant transformations over the preceding three industrial revolutions, moving from traditional farming to mechanised farming and, more recently, precision agriculture. Although the industrial farming paradigm significantly increases production, a number of issues have slowly surfaced and become worse recently. It is anticipated that Industry 4.0 will propel the fourth agricultural revolution and once again transform the agriculture sector. The current state of industrial agriculture is reviewed in this study, along with the lessons that may be drawn from industrialised agricultural production methods, industrialised agricultural production patterns, and the industrialised agri-food supply chain.

In addition, five cutting-edge technologies are explored in relation to Agriculture 4.0: blockchain, robots, artificial intelligence, big data analytics, and the Internet of Things. We specifically concentrate on the major uses of these cutting-edge technologies in the field of agriculture and the associated research difficulties. The purpose of this study is to introduce readers, especially industry practitioners, to new avenues for research. While earlier research has concentrated on one or up to four related enablers, we take a look at ten technological enablers, which include the frequently mentioned Big Data, Internet of

Things, and Cloud Computing as well as less common ones like Fog and Mobile Computing, Artificial Intelligence, Human-Computer Interaction, Robotics, and Open-Source Software, Blockchain, and the Internet. We examine the key features of each in light of I4.0 and its dependency on other enablers. Lastly, we offer a thorough examination of the difficulties in utilising each of I4.0's enablers, highlighting potential obstacles that may need to be surmounted and suggesting potential lines of inquiry for further study. Our objective is to serve as a reference for both laypeople seeking a high-level understanding of the variety (and frequently lengthy history) of the scientific research supporting Industry 4.0 and experts in some of the technological fields involved in exploring integration and hybridization possibilities with other fields.

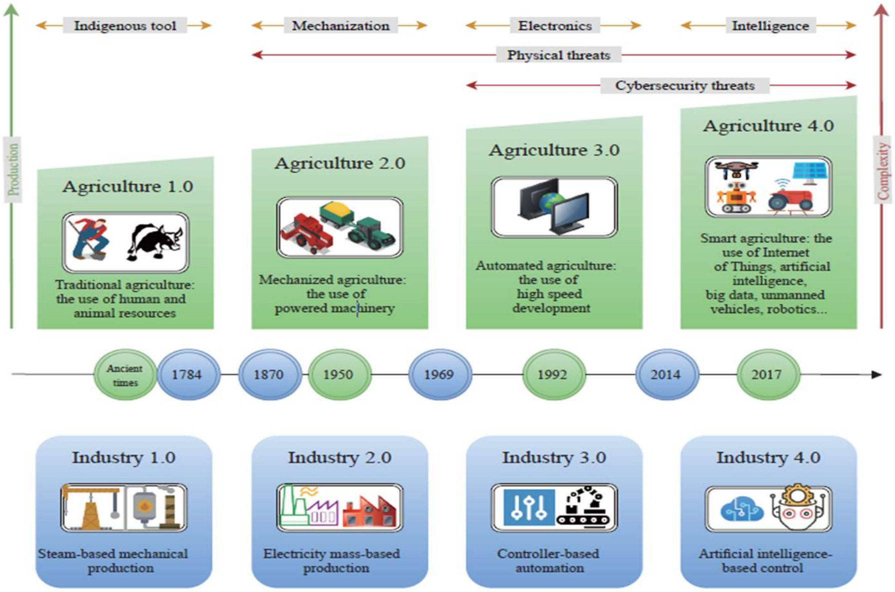

Indigenous tool
Mechanization
Electronics
Intelligence
Physical threats
Cybersecurity threats
Production
Complexity
Agriculture 1.0
Traditional agriculture: the use of human and animal resources
Agriculture 2.0
Mechanized agriculture: the use of powered machinery
Agriculture 3.0
Automated agriculture: the use of high speed development
Agriculture 4.0
Smart agriculture: the use of Internet of Things, artificial intelligence, big data, unmanned vehicles, robotics...
Ancient times
1784
1870
1950
1969
1992
2014
2017
Industry 1.0
Steam-based mechanical production
Industry 2.0
Electricity mass-based production
Industry 3.0
Controller-based automation
Industry 4.0
Artificial intelligence-based control

Figure 1. The Development Of Agricultural Revolutions With Industrial Revolutions And Related Cyber Security Threats.

As shown in Fig. 1, the agricultural and industrial revolution has progressed through four generations: Agriculture 1.0, Agriculture 2.0, Agriculture 3.0, and Agriculture 4.0. Agriculture 1.0 describes agricultural practises from the dawn of human civilization until the end of the 19th century, when farmers mainly relied on archaic farming implements like the plough to prepare the ground for planting seeds and growing plants. The rise in agricultural output at the start of the 20th century was dubbed "Agriculture 2.0" because it made use of trucks, tractors, aeroplanes, helicopters, irrigation, harvesting, combines, and other agricultural gear. Agriculture 3.0, which is centred on renewable green energy sources including geothermal, solar, wind, hydropower, and bioenergy, emerged in the early 1970s and continues to this day [1].

2.RELATED WORK

Cyberattacks are increasingly targeting Critical National Infrastructures (CNIs), which include ports, gas and water distributors, hospitals, and energy suppliers. CNIs primarily rely on Industrial Control Systems (ICS), also known as Supervisory Control and Data Acquisitions (SCADA), to oversee their production. The protection of ICSs and CNIs is now a crucial problem that needs to be taken into account at the national, international, and organisational levels. For example, Europe has produced several laws and legislation in recent years to try to build a logical framework for safeguarding networks, information, and electronic communications in order to deal with the growing risk of CNIs. To address the legal, organisational, capacity-building, and technological components of cyber security, particular security measures are also required in addition to rules, directives, and policies [1].

Systems with intrusion detection systems (IDS) [2] make up a system's second line of defence. To further protect the systems from cyberattacks, IDSs may be used in conjunction with other security measures including access control, authentication procedures, and encryption techniques. IDSs are able to differentiate between malicious and benign activity by using rules that specify a particular attack or patterns of benign traffic [3]. Data mining, which is used to characterise knowledge discovery, can assist in the development and deployment of intrusion detection systems (IDSs) with more accuracy and resilient behaviour in contrast to traditional IDSs, which might not be as successful against contemporary sophisticated cyberattacks [5].

Industry 4.0 has made extensive use of these cutting-edge technologies, and it is simple to mimic their use in agricultural settings. Therefore, since the deployment of thousands of IoT-based devices is in an open field, the main problem in establishing Agriculture 4.0 lies not in the deployment of future technologies but rather in ensuring security and privacy. Every layer of the IoT architecture also has a number of security and privacy concerns [6]. For instance, a hostile party might use a variety of cyberattacks, such as distributed denial-of-service (DDoS) assaults, to bring down a service and subsequently introduce fake data, so compromising agricultural production, food safety, and the effectiveness of the agri-food supply chain. The intrusion detection system (IDS) is a technology for network security that is devoted to continuously monitoring events within a computing or networking system and comparing them to intrusion evidence. It is recommended for use by the cyber security research community [7]. The use of the IDS in conjunction with other security technologies, including as blockchain, authentication, authorization, and encryption approaches, can further safeguard Agriculture 4.0 against cyberattacks [9].

Numerous related papers that address machine learning methods for intrusion detection systems can be found in the literature. The studies are categorised according to the following criteria, as shown in Table I:
Deep learning techniques: this indicates whether or not the study's emphasis was on deep learning techniques for intrusion detection systems. It shows whether or not machine learning techniques for intrusion detection systems were taken into account in the study. Assessment of deep learning techniques: it signifies if the research assesses deep learning techniques for intrusion detection systems. Assessment of machine learning techniques: it signifies if the research assesses machine learning techniques for intrusion detection systems.

Intrusion detection system (IDS) datasets: this shows if the study's focus was on these datasets.

Ring et al. [14] just published their work on intrusion detection datasets. The study specifically offers 34 datasets and defines 15 traits for each of them. General Information, Evaluation, Recording Environment, Data Volume, Nature of the Data, and General Information are the five areas into which these attributes are divided. A study of the machine learning techniques employed by intrusion detection systems was published by Buczak et al. [8]. The datasets in this study were divided into three categories: 1) packet-level data; 2) network flow data; and 3) public datasets. Furthermore, the study offered a computational complexity—that is, a time complexity—for every machine learning and mining technique that the intrusion detection system employed. A comparative analysis of intrusion detection techniques in the internet of things (IoT) was presented by Zarpelao et al. [11]. IDSs for IoT were categorised in the study according to security threat, IDS installation method, and detection strategy. Milenkoski et al. [9] examined current systems in relation to each of the common assessment parameters—workloads, metrics, and technique—to give common practises in cyber security intrusion detection. Our research and four other papers concentrate on deep learning techniques intended for the identification of cyber security intrusions. These publications, however, do not provide a dataset-by-dataset comparison of deep learning algorithms. To the best of our knowledge, this is the first research to compare deep learning for intrusion detection systems and to cover techniques, datasets, and other aspects in detail.

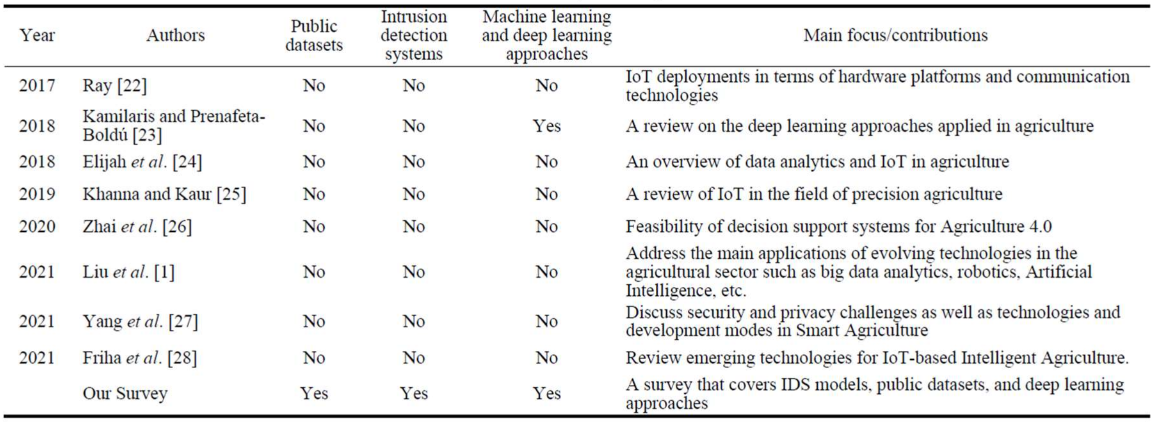
ABCIS

ABCIS is the combination of **A**rtificial Intelligence, **B**lockchain Technology, **C**loud computing, **I**oT and **S**oftware Defined Networks (SDN) and it is an emerging technology.

Industry 4.0, which is defined by a confluence of emerging technologies like Blockchain, software-defined networking (SDN), artificial intelligence, Internet of Things (IoT), IoT devices, 5G communications, drones, fog/edge computing, cloud computing, network function virtualization (NFV), smart grids, etc., preceded the term "Agriculture 4.0" [2], [3]. Fig. 1 displays the Agriculture 4.0 diagram. In the physical layer, a range of IoT devices (such as sensors and cameras) and drones are used to gather data on soil moisture, crop images, animal behaviour analysis, and health monitoring in order to monitor agricultural environmental conditions.

When the data fulfils certain criteria, various actuators (such as autonomous tractors, insecticidal lights, feeding machines, and irrigation equipment) are turned on, which encourages the automation of agricultural production and management. In addition, smart grid architecture and new energy technologies like solar and wind power help supply energy for IoT devices in Agriculture 4.0 [4]. Intelligent agriculture devices use the wireless network to send data to the Edge/Fog node and sink node at the network layer. This creates a variety of networks, such as the mesh network (based on ZigBee), the star network (based on LoRa), the GSM network (4G/5G based), and SDN (which includes control and data panes) [5]. Application-layer cloud computing is used to analyse data stored in a distributed database to help in decision-making related to agriculture production and management. Higher timeliness task implementation is achieved through the usage of edge/fog computing. Furthermore, a Smart Grid's electrical equipment operating status is often tracked by the supervisory control and data acquisition (SCADA) system.

Table 1. Related Surveys On Agriculture 4.0



Year	Authors	Public datasets	Intrusion detection systems	Machine learning and deep learning approaches	Main focus/contributions
2017	Ray [22]	No	No	No	IoT deployments in terms of hardware platforms and communication technologies
2018	Kamilaris and Prenafeta-Boldú [23]	No	No	Yes	A review on the deep learning approaches applied in agriculture
2018	Elijah *et al.* [24]	No	No	No	An overview of data analytics and IoT in agriculture
2019	Khanna and Kaur [25]	No	No	No	A review of IoT in the field of precision agriculture
2020	Zhai *et al.* [26]	No	No	No	Feasibility of decision support systems for Agriculture 4.0
2021	Liu *et al.* [1]	No	No	No	Address the main applications of evolving technologies in the agricultural sector such as big data analytics, robotics, Artificial Intelligence, etc.
2021	Yang *et al.* [27]	No	No	No	Discuss security and privacy challenges as well as technologies and development modes in Smart Agriculture
2021	Friha *et al.* [28]	No	No	No	Review emerging technologies for IoT-based Intelligent Agriculture.
	Our Survey	Yes	Yes	Yes	A survey that covers IDS models, public datasets, and deep learning approaches

Industry 4.0 has made extensive use of these cutting-edge technologies, and it is simple to mimic their use in agricultural settings. Therefore, since the deployment of thousands of IoT-based devices is in an open field, the main problem in establishing Agriculture 4.0 lies not in the deployment of future technologies but rather in ensuring security and privacy. Every layer of the IoT architecture also has a number of security and privacy concerns [6]. For instance, a hostile party might use a variety of cyberattacks, such as distributed denial-of-service (DDoS) assaults, to bring down a service and subsequently introduce fake data, so compromising agricultural production, food safety, and the effectiveness of the agri-food supply chain. The intrusion detection system (IDS) is a technology for network security that is devoted to continuously monitoring events within a computing or networking system and comparing them to intrusion evidence. It is recommended for use by the cyber security research community [7], [8]. The use of the IDS in conjunction with other security technologies, including as blockchain, authentication, authorization, and encryption approaches, can further safeguard Agriculture 4.0 against cyberattacks [9].

Table 2. Related Surveys on the IDSs Based on Machine Learning Techniques

Year	Authors	Taxonomy	IDS building process for Agriculture 4.0	Public datasets	Benefits of IDS for Agriculture 4.0	Open challenges and future research opportunities for Agriculture 4.0
2016	Buczak and Guven [10]	- Machine learning techniques	No	Partial	No	No
2019	Kwon *et al.* [11]	- Deep learning techniques	No	No	No	No
2020	Al-Garadi *et al.* [12]	- Deep learning techniques	No	No	No	No
2019	Mishra *et al.* [13]	- Machine learning techniques	No	Yes	No	No
2019	da Costa *et al.* [14]	- Machine learning techniques	No	Partial	No	No
2019	Chaabouni *et al.* [15]	- IoT threats classification	No	Yes	No	No
2019	Liu and Lang [16]	- Machine learning and deep learning techniques	No	No	No	No
2019	Sultana *et al.* [17]	- SDN	No	No	No	No
2020	Ahmad *et al.* [18]	- SDN	No	No	No	No
2020	Ferrag *et al.* [9]	- Deep learning techniques	No	Yes	No	No
2021	Ahmad *et al.* [19]	- Machine learning and deep learning techniques	No	No	No	No
2021	Mohammadi *et al.* [20]	- Support vector machines	No	No	No	No
	Our survey	- Cloud computing-enabled Agriculture 4.0	Yes	Yes	Yes	Yes
		- Fog/Edge-enabled Agriculture 4.0				
		- SDN/NFV-enabled Agriculture 4.0				
		- Drones-enabled Agriculture 4.0				
		- Autonomous tractors-enabled Agriculture 4.0				
		- IoT devices-enabled Agriculture 4.0				
		- Industrial Agriculture 4.0				
		- Smart Grid-enabled Agriculture 4.0				

Artificial intelligence-based methods, including hybrid machine learning, voting-based extreme learning machines, deep learning techniques, hierarchical approaches, reinforcement learning, etc., are used by IDSs to identify harmful behaviours. The machine learning-based IDSs have been the subject of several surveys. The relevant surveys on machine learning-based IDSs are shown in Table I. IDSs based on machine learning methods deep learning approaches [11], and [12] were the subject of several surveys. SCADA systems , SDN technologies and IoT networks [14], [15] were the subjects of certain surveys. This survey, on the other hand, suggests seven taxonomies pertaining to Agriculture 4.0 (cloud computing enabled), Agriculture 4.0 (fog/edge enabled), Agriculture 4.0 (SDN/NFV enabled), Agriculture 4.0 (drone enabled), Agriculture 4.0 (autonomous tractor enabled), Agriculture 4.0 (IoT device enabled), Agriculture 4.0 (industrial agriculture enabled), and 8) Agriculture 4.0 (smart grid enabled). Furthermore, by addressing innovative security themes including the IDS development process, public datasets, advantages of IDS, open problems, and future research potential for Agriculture 4.0, it offers a more thorough review.

3. CYBER SECURITY

While Agriculture 4.0 is meant to be the new norm, certain risks might limit its popularity and prevent it from being widely adopted. Some of those hazards, like severe weather, have a history of continuing over time. While others are linked to the widespread advancement of technical solutions, which have led to significant security flaws and dangerous attack vectors like ransomware, supply chain assaults, Internet of Things attacks, and several others.

Cyber Security Threats in Agriculture 4.0

For precision agriculture, the U.S. Department of Homeland Security identified three main areas of cyber threats: those pertaining to availability, confidentiality, and integrity.

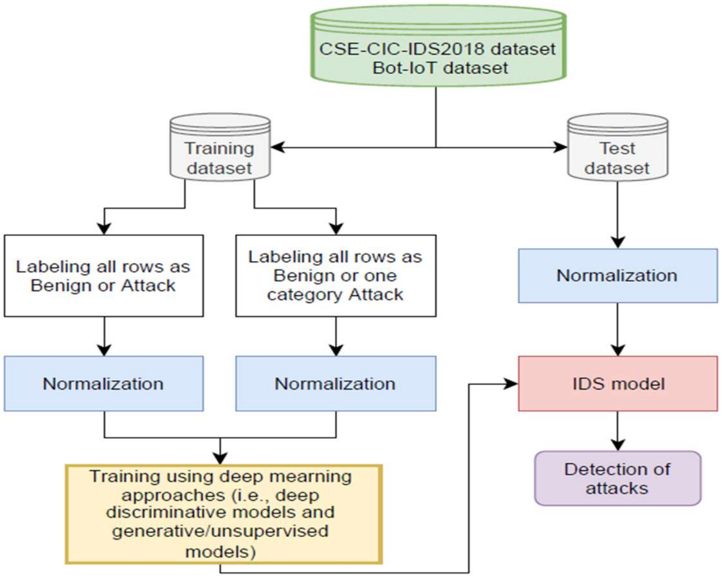

CSE-CIC-IDS2018 dataset
Bot-IoT dataset
Training dataset
Test dataset
Labeling all rows as Benign or Attack
Labeling all rows as Benign or one category Attack
Normalization
Normalization
Normalization
IDS model
Detection of attacks
Training using deep mearning approaches (i.e., deep discriminative models and generative/unsupervised models)

Figure 2. Flowchart Of The IDS Methodology.

Threats to Confidentiality: In intelligent agriculture, data travels from one linked equipment to another via a multitude of communication methods. Threats to privacy can result in data or information breaches as well as privacy loss [29]. Information on yields, farmland values, and animal health, for example, should be kept private as farmers are fiercely protective of this information. Farmers may suffer severe financial, emotional, and reputational repercussions if they misplace or misuse this data.

2) Threats to Integrity: To assist farmers in making wise management decisions in real time, gathering and using data is a crucial first step. Information from Intelligent Agricultural Systems may become erroneous or unreliable due to potential unauthorised or improper changes to the dependability of data or resources, which may lead to potential financial exploitation.

Threats Related to Availability: Inability to offer clients accessible services may result in disruptions to business operations, as well as a potential loss of clientele and revenue. For instance, food security would be disrupted and the equipment maker would suffer a significant loss of reputation if an attacker were to halt the operations of an already-existing Intelligent Agriculture Network.

An IDS's efficacy and efficiency may be assessed using a variety of measures, the majority of which fall into one of two categories: performance-based metrics or security-based metrics.

1) Metrics Based on Security: The efficacy of the IDS in differentiating between invasive and non-intrusive activities is described by the metrics in this area. Since an IDS is a binary classifier, its outputs can be any of the following: True positive (TP) refers to an intrusion that is correctly classified as an intrusive action; true negative (TN) is the proper classification of a legitimate action as legitimate; false positive (FP) refers to the incorrect classification of a legitimate action as an intrusion; and false negative (FN) refers to the incorrect classification of an intrusion as a legitimate action [31]. Among the well-known measures in this area are:

Confusion matrix: This measure shows the classification's outcome. For example, it displays the classification's true and false findings. When it comes to binary classification, it can have dimensions; but, when it comes to multi-class classifiers with distinct classes, it can also have dimensions. The confounding matrix is a baseline of metrics from which other efficacy indicators can be measured, even though it is not a metric in and of itself.

4. IDS SOLUTIONS FOR AGRICULTURE 4.0

Numerous cutting-edge technologies are used in agriculture 4.0, including cloud computing, fog/edge computing, SDN/NFV, drones, IoT devices, smart grids, and autonomous tractors.

We examine and analyse the IDSs that employ machine learning and deep learning approaches for cyber security in Agriculture 4.0 based on these new technologies.

Because Agriculture 4.0 uses a variety of IoT devices, there are a lot of new vulnerabilities in the cloud environment because these devices are easily targeted by security assaults. Three kinds of IDSs are available for Cloud computing-enabled Agriculture 4.0: 1) Game theory-based, 2) Hybrid machine learning, and 3) Voting based extreme learning machine.

The GTM-CSec model is built on three approaches: the signature, anomaly, and honeypot techniques. It consists of two basic components: cooperative and non-cooperative games.

The four components that use these procedures are perception, logical analysis, computational analysis, and decisive analysis. The analysis of the GTM-CSec model's performance using reward functions and probabilities in MATLAB demonstrated that it is highly effective at deterring attacks and can enhance the defence mechanism's electricity consumption.

2) Hybrid Machine Learning: Rabbani et al. [6] developed a hybrid machine learning system that is based on extracting users' behavioural patterns to identify dangerous behaviours in the cloud computing environment. This system is based on tracking user patterns of behaviour. The suggested approach makes use of particle swarm optimization-based probabilistic neural networks (PSO-PNN) to build an automatically optimised network. The UNSW-NB15 dataset was utilised in the study, and it contains characteristics that are provided in both qualitative and quantitative (i.e., numerical and symbolic) formats. According to the testing results, the PSO-PNN technique has a high degree of accuracy when it comes to identifying suspicious activity.

3) Voting Based Extreme Learning Machine: Kushwah and Ranga [7] examined a cloud infrastructure that has a detector connected. The infrastructure is composed of three parts: a training database, a preprocessor, and a classifier. As shown in Fig. 4, the detector recognises DDoS threats in a cloud computing context using a voting extreme learning machine. The NSL-KDD dataset and the ISCX dataset were the two datasets used in the investigation. The suggested approach offers excellent accuracies of 99.18% and 92.11% with the NSL-KDD and ISCX datasets, respectively, according to the experimental findings.

Using online multivariate statistical change analysis, Aldribi et al. [8] created an intrusion detection system (IDS) based on a hypervisor to identify unusual cloud behaviour. The study validated the suggested cloud intrusion detection methodology using the ISOT-CID dataset. According to the experimental findings, the suggested system has a 96.23% overall detection rate and a 7.56% false-positive rate.

Based on the Industrial Control System Cyber attack Dataset, the RSL-KNN framework system demonstrated 91.07% and 96.73% detection accuracies under multi-class and binary class classification, respectively, according to the performance evaluation.

Fig. 7 illustrates how blockchain technology and machine learning-based IDSSs are used to provide Agriculture 4.0 cyber security.

Zhou et al. [5] presented an IDS based on feature selection and ensemble classifier approaches that may be used for SDN/NFV-based Agriculture 4.0. A heuristic algorithm is employed to reduce dimensionality. For attack recognition, classifier approaches such as Random Forest and C4.5 are employed.

In the experimental phase, Weka 3.8.3 is utilised with the NSL-KDD, AWID, and CIC-IDS2017 datasets. The findings indicate that the suggested method achieves detection accuracy of 98.3% and 99.3% for C4.5 and Random Forest classifiers, respectively. An intrusion detection method called KPCA-DEGSAHKELM was developed by Lv et al. [66] using an extreme learning machine with a hybrid kernel function. This method may be employed for SDN/NFV-based Agriculture 4.0. The KPCA-DEGSAHKELM system, a hybrid method that combines the differential evolution algorithm with the gravitational search algorithm, is used to identify threats. The industrial intrusion detection dataset, UNSW-NB15 dataset, and KDD99 dataset are used to evaluate performance. The results demonstrate that the KPCA-DEGSA-HKELM system can achieve greater computational efficiency with savings of 82.21%.

Velliangiri and Karthikeyan [7] developed a hybrid optimisation strategy based on adaptive artificial bee colony optimisation and adaptive particle swarm optimisation techniques to increase the rate of precision in incursion operations. Four steps make up the hybrid optimisation scheme: i) selecting the dataset; ii) preprocessing the data; iii) selecting a feature; and iv) hybrid categorization. When compared to naive bayes and the support vector machine, the hybrid optimisation scheme's accuracy increases to 94.23% and 97.85%, respectively, according to the performance evaluation on the NSL-KDD dataset.

The internet of drones (IoD) has arisen as a new study subject of "drone-to-drone communication (D2D)" for the Agriculture 4.0 due to the integration of 5G systems in the burgeoning smart city concept [74]. In agriculture, the employment of many UAVs working together to accomplish a particular objective has enhanced production and decreased operating efforts . However, these systems are susceptible to cyberattacks, which an adversary may use to their advantage by stealing sent goods, gaining control of the system, or creating major disruptions.

Thus, it is becoming more and more important to ensure system security, particularly in dynamic and decentralised drone-to-drone networks. Therefore, the discovery of an IDS for Agriculture 4.0 remains very desirable.

Artificial Bee Colony (ABC) Model-Based

Cyber Agriculture 4.0, in which an adversary asserts several illicit identities by building or destroying IoT nodes, may face significant challenges as a result of the Sybil assault. A lightweight IDS based on the ABC model was presented by Murali and Jamalipour to detect the Sybil attack in the IoT context. The ABL model is employed as an optimisation method to mimic honey bee foraging behaviour. According to the simulation findings, the suggested IDS has an average accuracy rate of 96.8%, 95.2%, and 94.8% for type 1, type 2, and type 3 attacks, respectively. Malicious nodes in the type 1 assault will focus on a single, specific location. Type 2 attacks are made up of malicious nodes strewn throughout the genuine nodes, whilst type 3 attacks are made up of mobile Sybil nodes dispersed around the network. The work of Lopez-Martin et al. [10], in which the authors utilise reinforcement learning to network intrusion detection utilising two datasets, namely NSL-KDD and AWID datasets, can be applied to handle intrusion detection in supervised issues. The study assessed how well the IDS model performed while using the double deep Q-network (DDQN), policy gradient (PG), actorcritic (AC), and deep Q-network (DQN) deep reinforcement learning techniques. When compared to other deep reinforcement learning algorithms, the DDQN method performed well.

5. PUBLIC DATASETS

To increase the sector's efficiency, the food business has seen a transition from highly networked, dependent, and independent operations to disconnected, stand-alone, and independent operations [8]. Network organisations are thus placed in a highly effective production system that is becoming more complicated and exposed to dangers. As seen in Fig. 12, connectivity in the agri-food chain includes the management of information assets, the movement of tangible and intangible commodities and services, and other assets. It is getting harder and harder to secure all of the resources in the agriculture sector as a result of the widespread and pervasive nature of this control in Agriculture 4.0. We provide the Agriculture 4.0 IDS construction process in this part.

Data Preprocessing:

The data are initially processed to produce basic characteristics when they are acquired during the data collecting stage [4]. The feature selection approach, which is a pre-processing stage in machine learning algorithms, aims to improve or even maintain the IDS's performance while reducing the computational cost of the computations by eliminating superfluous characteristics [5]. Every record in the input data must be written as a real number vector in order for the trained classifier to function. As a result, a process known as data transferring must be used to first translate each symbolic feature in the dataset into a numerical value. Data normalisation is the practise of scaling each attribute's value over a proportionate range to eliminate bias towards larger-valued features in the dataset. This can greatly improve the classification algorithm's performance. In order to overcome the difficulty of creating an intrusion detection framework from imbalanced intrusion datasets that is especially intended for the industrial control system (ICS) and appropriate for use in Agriculture 4.0, Khan et al. [7] suggested a technique termed HMLIDS. The method uses a modified nearest-neighbor rule algorithm to balance the dataset and a feature extraction methodology built from data normalisation with data feature retrieval (DFR), which improved the classifiers' accuracy. A 97% accuracy rate was demonstrated in experimental findings derived from a large-scale actual dataset generated with a SCADA system.

Because developing technologies can integrate real-time data flow, historical data archives, and a variety of independent data analysis patterns, they enable more intelligent management of agri-food supply chains. In Agriculture 4.0, real-time data and automated data processing technologies provide new means of reacting faster to situations that change. As seen in Fig. 12, the activities related to every agricultural component are automatically linked, from farm to fork, into the food chain using new technology. There are certain of these components that need the utilisation of different data sources. Not only do these data need to be there, but they also need to function properly in all systems.

Among the essential elements of Agriculture 4.0 are:

1) *Smart Farming Systems:* These systems are made to increase the effectiveness and quality of agricultural production by incorporating cutting-edge technologies into currently practised farming operations. Examples of these include intelligent crop and livestock monitoring, intelligent water management, intelligent disease management, intelligent harvesting, etc. With an emphasis on connecting items in the Internet of Things-based smart farm, it consists of various sensor and actuator kinds, unmanned aerial and ground vehicles, smart agricultural gear, and so on. Using installed intelligent gadgets, while keeping an eye on things, carrying out farm-related duties, and processing data.

2) *Transport Services:* These services manage the movement of agricultural goods from the point of origin to the kitchen of the client, covering the whole supply chain. It comprises several smart sensor types, GPS kits, and Internet of Vehicles (IoV) communications, which allow cars to talk to one other and to public networks via interfaces called vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). They make it possible to gather and share sensitive data on the state of agricultural payloads and road conditions in real time.

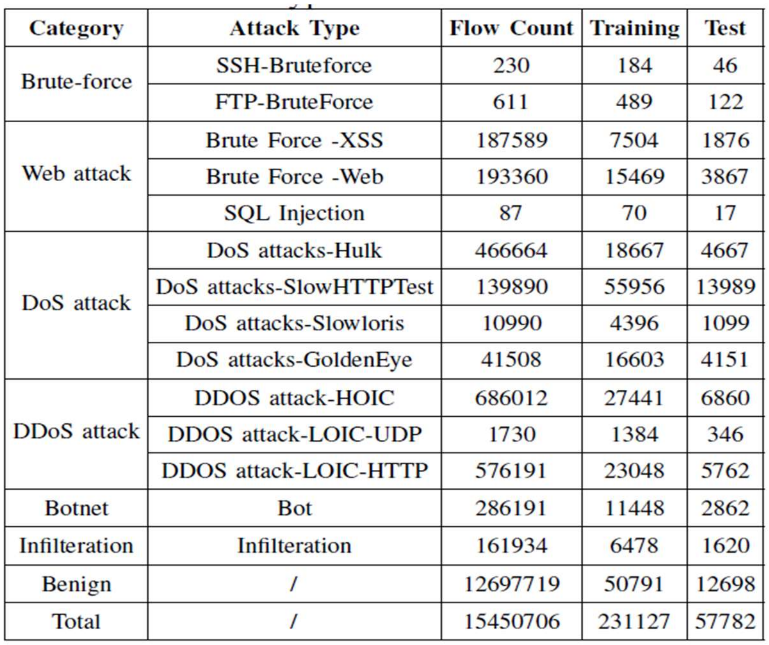
3) *Storage Entities:* These organisations oversee all aspects of storage management. Monitoring systems included into cold storage systems are able to track changes over time in the condition of the agricultural goods being stored, notifying and warning management as soon as something doesn't appear right. It consists of many kinds of smart sensors, including humidity and temperature sensors.

4) *Food processors:* These units produce prepared agricultural goods in addition to preparing fresh food for the market. It is made up of a sizable and varied collection of businesses that produce goods. In order to create their goods, they also employ agricultural raw materials or sub-assemblies made by other manufacturers. It is feasible to handle a variety of quality control tasks using IoT enabled equipment. Manufacturers may keep an eye on temperature and production levels for various commodities, as well as pressure levels and product labelling.

5) *Distributors:* These services often comprise an organisation that buys big stocks of goods from manufacturers and resells them to customers. Distributors provide the items to customers whenever and wherever they choose, satisfying the "Time and Place" criteria.

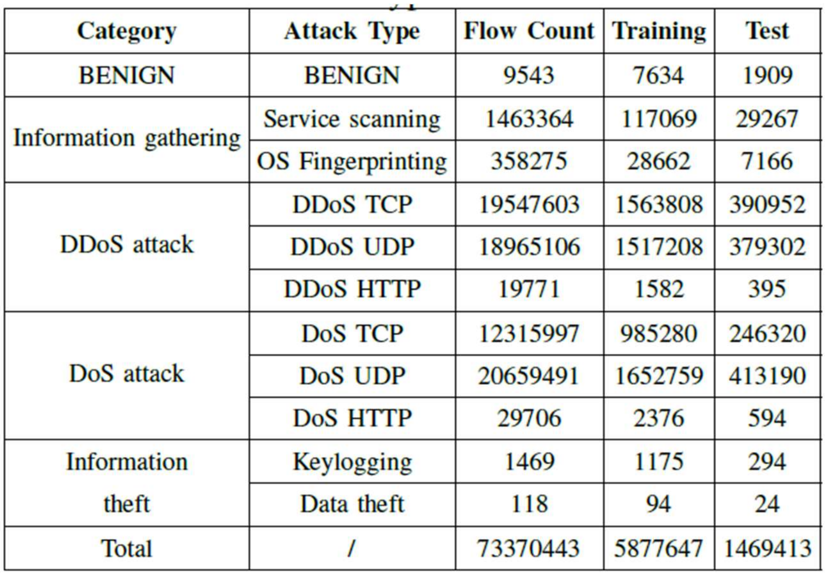
6) *Retailers:* These companies keep lesser quantities of inventory that they sell to the general public. They also monitor the tastes and needs of their clients.

Table 3. Attack Types In Cse-Cic-Ids2018 Dataset



Category	Attack Type	Flow Count	Training	Test
Brute-force	SSH-Bruteforce	230	184	46
	FTP-BruteForce	611	489	122
Web attack	Brute Force -XSS	187589	7504	1876
	Brute Force -Web	193360	15469	3867
	SQL Injection	87	70	17
DoS attack	DoS attacks-Hulk	466664	18667	4667
	DoS attacks-SlowHTTPTest	139890	55956	13989
	DoS attacks-Slowloris	10990	4396	1099
	DoS attacks-GoldenEye	41508	16603	4151
DDoS attack	DDOS attack-HOIC	686012	27441	6860
	DDOS attack-LOIC-UDP	1730	1384	346
	DDOS attack-LOIC-HTTP	576191	23048	5762
Botnet	Bot	286191	11448	2862
Infilteration	Infilteration	161934	6478	1620
Benign	/	12697719	50791	12698
Total	/	15450706	231127	57782

Table 4. Attack Types In Bot-Iot Dataset



Category	Attack Type	Flow Count	Training	Test
BENIGN	BENIGN	9543	7634	1909
Information gathering	Service scanning	1463364	117069	29267
	OS Fingerprinting	358275	28662	7166
DDoS attack	DDoS TCP	19547603	1563808	390952
	DDoS UDP	18965106	1517208	379302
	DDoS HTTP	19771	1582	395
DoS attack	DoS TCP	12315997	985280	246320
	DoS UDP	20659491	1652759	413190
	DoS HTTP	29706	2376	594
Information theft	Keylogging	1469	1175	294
	Data theft	118	94	24
Total	/	73370443	5877647	1469413

The probability of any joint configuration may be computed using the Gibbs distribution and this energy function in the following ways:

$$Prob(V,H,G) = -\frac{1}{Z(G)}e^{-En(V,H,G)}$$

where Z, the partition function, can be computed in the manner described below:

$$Z(G) = \sum_{V\in\mathcal{V}}\sum_{H\in\mathcal{V}} e^{-En(V,H,G)}$$

where the space of the visible and hidden units is represented by the curved letters V and V, respectively.

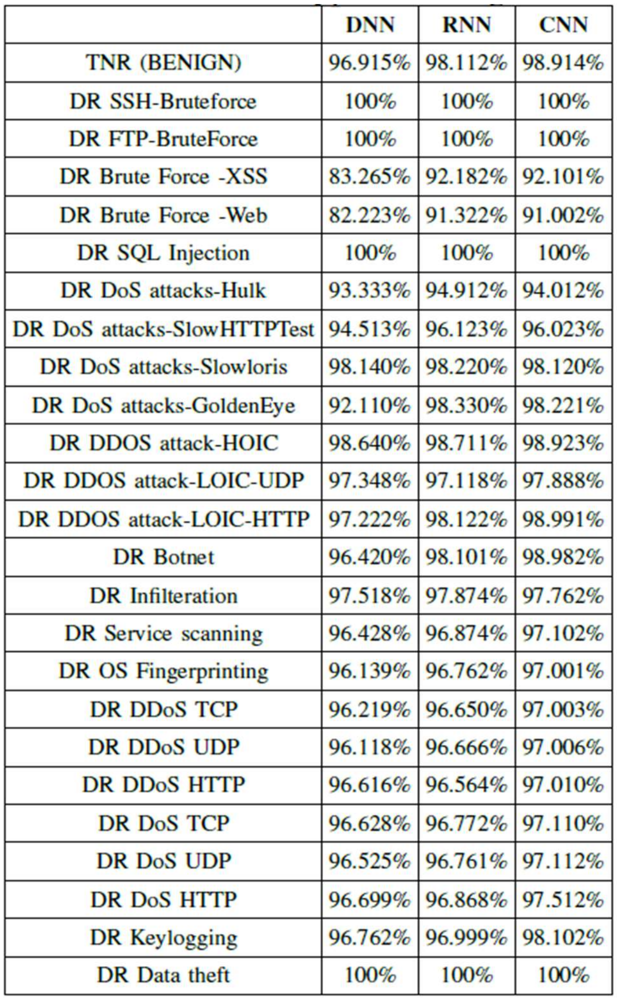
Performance metrics

$$DR_{Attack} = \frac{TP_{Attack}}{TP_{Attack}+FN_{Attack}}$$

$$TNR_{BENIGN} = \frac{TN_{BENIGN}}{TN_{BENIGN}+FP_{BENIGN}}$$

$$FAR = \frac{FP_{BENIGN}}{TN_{BENIGN}+FP_{BENIGN}}$$

Table 5. Deep Discriminative Models' Performance In Relation To Various Assault Types And Benign



	DNN	RNN	CNN
TNR (BENIGN)	96.915%	98.112%	98.914%
DR SSH-Bruteforce	100%	100%	100%
DR FTP-BruteForce	100%	100%	100%
DR Brute Force -XSS	83.265%	92.182%	92.101%
DR Brute Force -Web	82.223%	91.322%	91.002%
DR SQL Injection	100%	100%	100%
DR DoS attacks-Hulk	93.333%	94.912%	94.012%
DR DoS attacks-SlowHTTPTest	94.513%	96.123%	96.023%
DR DoS attacks-Slowloris	98.140%	98.220%	98.120%
DR DoS attacks-GoldenEye	92.110%	98.330%	98.221%
DR DDOS attack-HOIC	98.640%	98.711%	98.923%
DR DDOS attack-LOIC-UDP	97.348%	97.118%	97.888%
DR DDOS attack-LOIC-HTTP	97.222%	98.122%	98.991%
DR Botnet	96.420%	98.101%	98.982%
DR Infilteration	97.518%	97.874%	97.762%
DR Service scanning	96.428%	96.874%	97.102%
DR OS Fingerprinting	96.139%	96.762%	97.001%
DR DDoS TCP	96.219%	96.650%	97.003%
DR DDoS UDP	96.118%	96.666%	97.006%
DR DDoS HTTP	96.616%	96.564%	97.010%
DR DoS TCP	96.628%	96.772%	97.110%
DR DoS UDP	96.525%	96.761%	97.112%
DR DoS HTTP	96.699%	96.868%	97.512%
DR Keylogging	96.762%	96.999%	98.102%
DR Data theft	100%	100%	100%

There are 15450706 rows in the CSE-CIC-IDS2018 dataset, distributed over 10 files, with 80 characteristics per row. The following is a description of the contents of these files:

File 1 "Wednesday-14-02-2018" has benign traffic (667626 rows), SSH-Bruteforce (187589 rows), and FTPBruteForce (193360 rows).
File 2 "Thursday-15-02-2018" has benign traffic (996077 rows), Slowloris (10990 rows) and GoldenEye (415008 rows) DoS assaults.
File 3 "Friday-16-02-2018" includes benign traffic (442020 rows), DoS attacks—Hulk (466664 rows), and SlowHTTPTest (139890 rows).
Estimated class bad class uplifting classroom bad class Actual negative (TN) Positive falsehood

(FP) uplifting lesson Negative falsehood (FN) A true positive (TP).

The file "Thursday-20-02-2018" comprises both benign traffic (7372557 rows) and DDOS attack-LOIC-HTTP (576191 rows).

File 5 "Wednesday-21-02-2018" includes benign traffic (360833 rows), DDOS attack-HOIC (68601 rows), and DDOS attack-LOIC-UDP (1730 rows).

Brute Force-XSS (79 rows), Brute Force-Web (249 rows), SQL Injection (34 rows), and innocuous traffic (1048213 rows) are all included in File 6 "Thursday-22-02-2018".

File 7 "Friday-23-02-2018" includes innocuous traffic (1048009 rows), Brute Force -XSS (151 rows), Brute Force -Web (249 rows), and SQL Injection (53 rows).

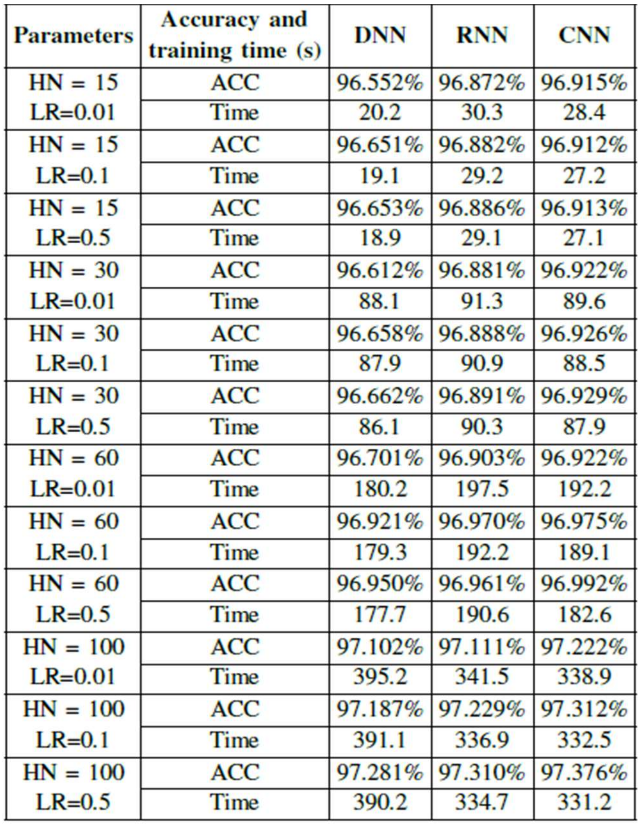
File 8 "Wednesday-28-02-2018" includes benign traffic (544200 rows) and an infiltration assault (68871 rows).

File 9 "Thursday-01-03-2018" has benign traffic (238037 rows) and an infiltration assault (93063 rows).

File 10 "Friday-02-03-2018" has benign traffic (762384 rows) and botnet attack (286191 rows).

More than 72.000.000 entries, divided among 74 files, with 46 characteristics per row, make up the BoT-IoT dataset. We employ the training and testing version that Koroniotis et al. [3] suggested, which uses 5% of the complete dataset. To generate a subset of training and testing, we use PyMongo 3.7.2 to import the files into a single JSON document.

Table 6. The CSE-CIC-IDS2018 Dataset's Deep Discriminative Models' Accuracy And Training Duration With Varying Learning Rates And Hidden Nodes.



Parameters	Accuracy and training time (s)	DNN	RNN	CNN

HN = 15
LR=0.01
	ACC	96.552%	96.872%	96.915%

	Time	20.2	30.3	28.4

HN = 15
LR=0.1
	ACC	96.651%	96.882%	96.912%

	Time	19.1	29.2	27.2

HN = 15
LR=0.5
	ACC	96.653%	96.886%	96.913%

	Time	18.9	29.1	27.1

HN = 30
LR=0.01
	ACC	96.612%	96.881%	96.922%

	Time	88.1	91.3	89.6

HN = 30
LR=0.1
	ACC	96.658%	96.888%	96.926%

	Time	87.9	90.9	88.5

HN = 30
LR=0.5
	ACC	96.662%	96.891%	96.929%

	Time	86.1	90.3	87.9

HN = 60
LR=0.01
	ACC	96.701%	96.903%	96.922%

	Time	180.2	197.5	192.2

HN = 60
LR=0.1
	ACC	96.921%	96.970%	96.975%

	Time	179.3	192.2	189.1

HN = 60
LR=0.5
	ACC	96.950%	96.961%	96.992%

	Time	177.7	190.6	182.6

HN = 100
LR=0.01
	ACC	97.102%	97.111%	97.222%

	Time	395.2	341.5	338.9

HN = 100
LR=0.1
	ACC	97.187%	97.229%	97.312%

	Time	391.1	336.9	332.5

HN = 100
LR=0.5
	ACC	97.281%	97.310%	97.376%

	Time	390.2	334.7	331.2

With 96.915%, it demonstrates that deep neural networks provide the highest true negative rate. For seven attack types, the recurrent neural network achieves the highest detection rate: 92.182% for Brute Force - XSS, 91.322% for Brute Force - Web, 94.912% for DoS attacks against Hulk, 96.123% for DoS attacks against SlowHTTPTest, 98.220% for DoS attacks against Slowloris, 98.330% for DoS attacks against GoldenEye, and 97.874% for Infilteration. The highest detection rate for four types of assaults is provided by the convolutional neural network: DDOS attack-HOIC 98.923%, DDOS attack-LOIC-UDP 97.888%, DDOS attack-LOIC-HTTP 98.991%, and Botnet 98.982%.

6. CONCLUSION

We examined and examined IDS for cyber security in Agriculture 4.0 in this research. We started by outlining the risks to cyber security and the various criteria used to assess an IDS's effectiveness for Agriculture 4.0. We then assessed IDSs in light of new technology. Furthermore, we provide a thorough categorization of IDSs in each developing technology. Next, we demonstrated the openly available datasets and implementation frameworks that are relevant to the Agriculture 4.0 IDS performance evaluation. In conclusion, we outlined the obstacles and potential avenues for further investigation in the field of intrusion detection for cybersecurity in Agriculture 4.0.

REFERENCES

[1] L. A. Maglaras, K.-H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz, "Cyber security of critical infrastructures," ICT Express, vol. 4, no. 1, pp. 42–45, 2018.

[2] A. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," International Journal of Communication Systems, vol. 31, no. 9, p. e3547, 2018.

[3] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," arXiv preprint arXiv:1812.09059, 2018.

[4] Z. Dewa and L. A. Maglaras, "Data mining and intrusion detection systems," International Journal of Advanced Computer Science and Applications, vol. 7, no. 1, pp. 62–71, 2016.

[5] Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.

[6] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in ICISSP, 2018, pp. 108–116.

[7] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, "Deep learning techniques for cyber security intrusion detection : A detailed analysis," in 6th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2019), Athens, 10-12 September, 2019.

[8] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2015.

[9] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," ACM Computing Surveys (CSUR), vol. 48, no. 1, p. 12, 2015.

[10] Ravindra Changala, A Novel Approach for Network Traffic and Attacks Analysis Using Big Data in Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering: 2320-9798, Volume 10, Issue 11, November 2022.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. J. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1646–1685, Apr. 2020.

[12] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," IEEE Commun. Surv. Tutor., vol. 21, no. 1, pp. 686–728, Feb. 2019.

[13] Ravindra Changala, AIML and Remote Sensing System Developing the Marketing Strategy of Organic Food by Choosing Healthy Food, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume 07 Issue 09, ISSN: 2582-3930, September 2023.

[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Commun. Surv. Tutor., vol. 21, no. 3, pp. 2671– 2701, Jan. 2019.

[15] H. Y. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019. DOI: 10.3390/app9204396.

[16] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.

[17] A. Ahmad, E. Harjula, M. Ylianttila, and I. Ahmad, "Evaluation of machine learning techniques for security in SDN," in Proc. IEEE Globecom Workshops, Taiwan, China, 2020, pp. 1−6.

[18] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, p. e4150, Jan. 2021.

[19] Ravindra Changala, Development of CNN Model to Avoid Food Spoiling Level, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN: 2456-3307, Volume 9, Issue 5, September-October-2023, Page Number 261-268.

[20] detection systems," J. Netw. Comput. Appl., vol. 178, p. 102983, Mar. 2021. DOI: 10.1016/j.jnca.2021.102983.

M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," J. Inf. Secur. Appl., vol. 52, p. 102500, Jun. 2020.

[21] S. Weyer, M. Schmitt, M. Ohmer, and D. Gorecky. Towards industry 4.0-standardization as the crucial challenge for highly modular, multivendor production systems. IFAC-PapersOnLine, 48(3):579–584, 2015.

[22]Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.

[23] Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Volume 12, Issue 16s), February 2024.

[24] Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, Volume 11, Issue 3), July 2023

[25] T. Goldschmidt, M. K. Murugaiah, C. Sonntag, B. Schlich, S. Biallas, and P. Weber. Cloud-based control: A multi-tenant, horizontally scalable soft-plc. In Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, pages 909–916. IEEE, 2015.

[26] Y. Liu and X. Xu. Industry 4.0 and cloud manufacturing: A comparative analysis. Journal of Manufacturing Science and Engineering, 139(3): 034701, 2017.

[27] Y. Hao and P. Helo. The role of wearable devices in meeting the needs of cloud manufacturing: A case study. Robotics and Computer-Integrated Manufacturing, 2015.

[28] Ravindra Changala ,"Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms And Classification Techniques", ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.

[29] Ravindra Changala "A Survey1 on Clustering Techniques to Improve Energy Efficient Routing in Wireless Sensor Networks" in International Journal of Applied Engineering Research ,10(58), pp.-1-5,2015.

[30] F. Tardieu, L. Cabrera-Bosquet, T. Pridmore, and M. Bennett, "Plant phenomics, from sensors to knowledge," Current Biology, vol. 27, no. 15, pp. 770–783, 2017.

[31] Z.-H. Zhan, X.-F. Liu, Y.-J. Gong, J. Zhang, H. S.-H. Chung, and Y. Li.Cloud computing resource scheduling and a survey of its evolutionary approaches. ACM Computing Surveys (CSUR), 47(4):63, 2015.

[32] Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, Volume 11, Issue 3), July 2023.

[33] N. Guiomar, S. Godinho, T. Pinto-Correia, M. Almeida, and F. Bartolini et al., "Typology and distribution of small farms in europe: Towards a better picture," Land Use Policy, vol. 75, pp. 784–798, 2018.

[34] J. W. Mellor and S. J. Malik, "The impact of growth in small commercial farm productivity on rural poverty reduction," World Development, vol. 91, pp. 1–10, 2017.

[35] Ravindra Changala, A Novel Approach for Network Traffic and Attacks Analysis Using Big Data in Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering: 2320-9798, Volume 10, Issue 11, November 2022.

[36] Ravindra Changala, MapReduce Framework to Improve the Efficiency of Large Scale Item Sets in IoT Using Parallel Mining of Representative Patterns in Big Data, International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 9, Issue 6, Page Number: 151-161, November 2022.

[37] Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.

[38] Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.

[39] M. Gautam and M. Ahmed, “Too small to be beautiful? the farm size and productivity relationship in bangladesh,” Food Policy, vol. 84, pp. 165–175, 2019.

[40] D. F. Larson, R. Muraoka, and K. Otsuka, “Why african rural development strategies must depend on small farms,” Global Food Security, vol. 10, pp. 39–51, 2016.

[41] G. Folino and P. Sabatino, “Ensemble based collaborative and distributed intrusion detection systems: A survey,” Journal of Network and Computer Applications, vol. 66, pp. 1–16, 2016.

[42] Ravindra Changala, A Novel Prediction Model to Analyze Evolutionary Trends and Patterns in Forecasting of Crime Data Using Data Mining and Big Data Analytics, Mukt Shabd Journal, Volume XI, Issue X, October 2022, ISSN NO: 2347-3150.

[43] X. Xu. From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing, 28(1):75–86, 2012.