Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Deep Learning Based Security Schemes for IoT Applications: A Review

Mina Farooq, Shavan Askar, Daban Ali Qadir, Media Ali Ibrahim, Nihad Abdullah
shavan.askar@epu.edu.iq, mina.othman@epu.edu.iq
Department of Information System Engineering, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq

Article Information

Submitted : 20 Mar 2024
Reviewed: 24 Mar 2024
Accepted : 8 Apr 2024

Keywords

Security, Applications, Internet of Things (IoT), Deep learning (DL), Machine Learning (ML).

Abstract

Due to its widespread perception as a crucial element of the Internet of the future, the Internet of Things (IoT) has garnered a lot of attention in recent years. The Internet of Things (IoT) is made up of billions of sentients, communicative "things" that expand the boundaries of the physical and virtual worlds. Every day, such widely used smart gadgets generate enormous amounts of data, creating an urgent need for rapid data analysis across a range of smart mobile devices. Thankfully, current developments in deep learning have made it possible for us to solve the issue tastefully. Deep models may be built to handle large amounts of sensor data and rapidly and effectively learn underlying properties for a variety of Internet of Things applications on smart devices. We review the research on applying deep learning to several Internet of Things applications in this post. Our goal is to provide insights into the many ways in which deep learning techniques may be used to support Internet of Things applications in four typical domains: smart industrial, smart home, smart healthcare, and smart transportation. One of the main goals is to seamlessly integrate deep learning and IoT, leading to a variety of novel ideas in IoT applications, including autonomous driving, manufacture inspection, intelligent control, indoor localization, health monitoring, disease analysis, and home robotics. We also go over a number of problems, difficulties, and potential avenues for future study that make use of deep learning (DL), which is turning out to be one of the most effective and appropriate methods for dealing with various IoT security concerns. The goal of recent research has been to enhance deep learning algorithms for better Internet of Things security. This study examines deep learning-based intrusion detection techniques, evaluates the effectiveness of several deep learning techniques, and determines the most effective approach for deploying intrusion detection in the Internet of Things. This study uses Deep Learning (DL) approaches to better expand intelligence and application skills by using the large quantity of data generated or acquired. The many IoT domains have drawn the attention of several academics, and both DL and IoT approaches have been explored. Because DL was designed to handle a variety of data in huge volumes and required processing in virtually real-time, it was indicated by several studies as a workable method for handling data generated by IoT.

Attribution-ShareAlike 4.0 International License

A. Introduction

With the rise of IoT technology, machine-to-machine and person -to-machine communication became more efficient and intelligent. Thus, smart items making life more pleasant and allowed us to control anything (Jose and Jose 2021). Using embedded devices, communication technologies, Internet protocols, data analytics, and more, IoT aims to make everyday items smart (Al-Fuqaha et al. 2015). IoT is predicted to provide various business possibilities and boost IoT-based service development. Based on McKinsey's IoT worldwide economic effect research (Manyika et al. 2013), the 2025 economic effect of IoT would be $2.7 to $6.2 trillion. Healthcare accounts for 41% of the IoT market, followed by industrial (33%), and energy (7%). Transportation, agriculture, urban infrastructure, security, and retail account for 15% of the IoT market. These predictions indicate rapid expansion of IoT services, data, and the linked industry in the next years (Banaamah and Ahmad 2022). Malicious actors may use this expansion to compromise data privacy, integrity, and availability. Cybersecurity protects data, privacy, and networks against illegal access. IoT security has become more important as more apps reliant on connected devices are created (Thakkar and Lohiya 2021),(Li et al. 2021). One of the hardest IT research areas is cybersecurity (Zhang et al. 2021),(Lee 2020). All parts of society are being affected by IoT and smart gadgets (Tahaei et al. 2020), such as smart hospitals, smart homes, intelligent vehicles, intelligent distributed networks (Pecori 2012), smart manufacturing industries, smart grids (Bonetto et al. 2020), and smart virtual learning environments (Pecori 2019). However, the broad use of such a disruptive technology raises security concerns due to the massive data streams from/to smart devices. Many IoT applications need security and precise authentication (Calabretta, Pecori, and Veltri 2018),(Calabretta, Pecori, Vecchio, et al. 2018) and classification techniques (Pecori et al. 2020) in turn, together with sufficient confidentiality and integrity measures. Due to the extensive usage of IoT devices, criminal acts might affect Internet security and strength. A particular botnet called 'Mirai' has recently affected widespread distributed denial of service (DDoS) assaults employing IoT equipment (Bertino and Islam 2017), (Kolias et al. 2017).(Bharati and Podder 2022). The Mirai virus (malware) (Perrone et al. 2017) is a clarified example of a cyber-attack. launched by the IoT (Perrone et al. 2017) illustrates the disruptive power of such harmful actions and the need for adequate countermeasures (Aversano et al. 2021). For any type of data use and flow between different devices and cloud storage. This decade's most contentious issues are mesh-up DL and IoT research evaluations. IoT devices pose security risks. Additionally, IoT stages generate a lot of relevant data. A serious privacy gap may arise if this information is not processed and transferred securely. Authentication, encryption, application security, network security, and access control are insufficient and difficult for large systems with many connected schemes. Everything on the IoT platform is vulnerable. There might be a number of causes for the privacy and security problems, including threats, assaults, and other weaknesses. Threats and weaknesses add up to create risk. Risk is the incapacity to prevent threats from destroying or damaging a system or information by taking advantage of the weakness. It is what happens when weaknesses and dangers combine. A system is at risk if it has threats and vulnerabilities. A purposeful or unintentional action mechanism that exploits a security flaw in the system to cause a security breach or adverse effect on it is called a threat (Abomhara and Køien 2015),(Alaba et al. 2017). Similarly, assaults may also have a significant negative effect on the security of the system by interfering with regular operations via the use of various tools and methods to exploit weaknesses. Information that has been altered, deleted, or removed without authorization poses a security risk. Assaults come in a variety of forms, including physical, denial-of-service, access, and privacy assaults (Abomhara and Køien 2015). Hardware, software, rules, and users may constitute vulnerabilities or liabilities. Hardware vulnerability linked to compatibility and interoperability is difficult to discover and remedy. Operating systems, applications, and controls have software weaknesses (Abomhara and Køien 2015). However, despite DL's remarkable achievements in a number of fields, many elements remain unexplained. When using complex and computationally costly deep learning algorithms, some simple DL techniques provide comparable outcomes. Whether transferability can help us clarify the features or hierarchies in deep learning models is still up for debate. Even if multiple DL models may provide comparable results from the same inputs, we are unable to attack different deep learning algorithms with the same evasion strategies. Stated differently, we may use these transferability features to safeguard DL models (Lin, 2020). DL is a branch of ML that translates discriminating or generative pattern analysis functions into abstractions utilizing different non-linear layers of computing. Since DL techniques have the potential to capture hierarchical pictures in deep architecture, they often identify as hierarchical learning techniques. The way that human neurons and the brain perceive impulses is what drives the operational theory of deep learning. In the last several years, DL has emerged as a crucial area of research for IoT systems (Li, Ota, and Dong 2018), (Shadroo, Rahmani, and Rezaee 2021), (Rahman and Hossain 2021). The major benefit of DL over standard machine learning is its performance on large datasets. IoT systems generate plenty of data, therefore DL approaches work well. Additionally, DL provides dynamic data representations (Liang et al. 2020). DL techniques allow for deep connectivity inside the IoT ecosystem. (Fadlullah et al. 2017). Deep connection is a single protocol that automates IoT computer and application communication. For instance, IoT gadgets automatically communicate to create a fully intelligent house (Li et al. 2018). DL techniques use a multi-layered computational paradigm to acquire varying levels of data structure abstraction. State-of-the-art procedures have been substantially advanced by DL techniques as compared to standard ML approaches (LeCun, Bengio, and Hinton 2015), (Bharati, Podder, and Mondal 2020)

B. Related Works

DL approaches depend on data sources. We need additional data to improve DL for IoT because to a scarcity of large datasets. IoT applications also struggle to create raw data for DL models. For better results, several DL algorithms need data preparation. IoT applications need extensive preprocessing because they deal with data from several sources with varying formats and distributions and missing data. Data collecting system use is a crucial research issue. The quantity and deployment of sensors affect data quality. Even with a good model design, you need a data gathering module for the complete IoT system. Model should be more dependable, cost-effective, and trustworthy. IoT security is the largest difficulty since we gather data from multiple sources. In many IoT applications, data privacy and confidentiality are key concerns since huge data is provided for review online, making it available globally. Some programs employ anonymization, although it may be abused and re-identified. Since DL models learn raw data features, they may profit from incorrect data streams. DL models must be updated utilizing approaches for irregular or faulty data. As shown in Table 1.

Table 1. Review Of Recent Surveys Concerning Deep Learning Approaches for IOT Security

Ref	Title	Publication Venue	Year	Syst. Review	DL Focused	IOT Focused	Datasets Description	No. Considered Attacks	Issues
(Kuruva Lakshmanna et al. 2022)	A Review on Deep Learning Techniques for IoT Data	Electronics	2018	No	Partially	Yes	No	It depends	Yes
(Hassaan Khalid et al. 2023)	A Brief Overview of Deep Learning Approaches for IOT Security	Elsevier	2023	No	Partially	Yes	YES	6	Yes
(Elsayed, Elsayed, and Bayoumi 2023)	IOT Botnet Detection Using an Economic Deep Learning Model	IEEE	2023	No	Partially	Yes	Yes	It depends	Yes
(Tang, Jie, Dawei Sun 2017)	Enable Deep Learning on IOT Devices	IEEE	2017	Yes	Partially	No	YES	1	Yes
(Alkahtani and Aldhyani 2021)	Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms	Elsevier	2021	Yes	Partially	No	YES	1	Yes
(Mohammadi et al. 2018)	Deep learning for IoT big data and streaming analytics: A survey	IEEE	2018	No	Partially	Yes	Yes	It depends	Yes
(Almutairi and Abdulghani Alshargabi 2022)	Using Deep Learning Technique to Protect Internet Network from Intrusion in IOT Environment	Elsevier	2022	No	Partially	Yes	Yes	5	Yes
(Banaamah and Ahmad 2022)	Intrusion Detection in IOT Using Deep Learning	Sensor	2022	No	Partially	Yes	Yes	It depends	Yes
(Bharati and Podder 2022)	Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions	Elsevier	2022	No	Partially	Yes	Yes	8	Yes
(Ma et al. 2019)	A survey on deep learning empowered IoT applications	IEEE	2019	No	Partially	Yes	Yes	It depends	Yes
(Salunkhe Madhav Jagannath et al. 2023)	Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems	Research Gate	2023	No	Partially	Yes	Yes	It depends	Yes
(Bakhsh et al. 2023)	Enhancing IoT network security through deep learning-powered Intrusion Detection System	Research Gate	2023	No	Partially	Yes	Yes	It depends	Yes

(Karne et al. 2022)	Applications of IoT on Intrusion Detection System with Deep Learning Analysis	Research Gate	2022	No	Partially	Yes	Yes	It depends	Yes

C. IoT Architecture

This section describes common IoT systems and their primary security risks. IoT revolutionized our civilization by turning ordinary objects into smart ones using technology for communication, protocols for the Internet and applications, and edge and ubiquitous computing paradigms (Al-Fuqaha et al. 2015). All IoT systems link many heterogeneous devices, which use machine-to-machine, human-to-human, and human-to-machine communication patterns(Alaba et al. 2017), Figure 1 depicts all IoT architectures. The graphic shows that IoT designs typically have three functional layers: perception or physical, network or communication, and application, which may be further divided. Each level is briefly described in the subsections that follow, with special attention paid to the specific sub-layers that each level may consist of.

This area's foundation is highlighting the overall quality of IoT systems as well as issues that may arise.

• Through connectivity via edge and cloud computing, the Internet of Things transforms civilization from a backward to a forward-thinking one.

• patterns of devices that enable heterogeneity, such as system to person, person to system, or system to system are intended to be changed and connected by Internet of Things technologies.

• IoT architectural pieces summarized in terms of the three OSI levels

a) Physical layers
b) Network layer
c) Application

and split even more (Al-Garadi et al. 2020).

3.1 Physical Layer: The physical layer's responsibility is to handle practical tasks including perception, data collection and processing, and evaluation.

• Action in the physical world is enabled via sensors and actuators.

• Bluetooth, IEEE, Wi-Fi, and NFC are needed for physical layer IoT connectivity.

IoT sensors have limited battery life and computational power, making them devices with restricted resources. A significant portion of large data and streams of big data (Pecori, Ducange, and Marcelloni 2019) This IoT layer is precisely what floods existing IT systems with data; yet, because these data are raw, accurately comprehending them is essential to creating a context-aware IoT system (Sethi, Sarangi, and others 2017). It is true that there are many advantages to having a solid grasp of the big data related to IoT, but this is often the responsibility of the application layer.

3.2 Network Layer: Because it coordinates data transfer across levels and bridges application and network layers, this layer may discover communication and computation difficulties.

The network layer is kindly regarded as the internet layer, hence certain problems occur while distributing internet connections:

• Give trillions of devices distinct IP addresses.

• IPv6 class-less addressing solved it.

- The size of the packets to be sent presented the second difficulty.
- The resolution was achieved by using precise internet protocol and the compression technique 6LoWPAN (Thubert et al. 2017). 32-bit address space to a 128-bit address space.

This layer includes middleware functions as well as communication capabilities. In reference to the former, it is still necessary to give serious thought to how limited IoT devices are. Giving each of the billions of Internet-connected smart gadgets a unique IP address is one of the biggest issues at this layer. Utilizing the IPv6 addressing method, this problem may be gradually eased. One other issue with network layer communications is the size of the packets being sent. This will be resolved by implementing appropriate protocols, such 6LoWPAN, that can provide timely compression capabilities. Routing functions are impacted by a third problem, which arises from the need for routing protocols to enable the mobility and flexibility of smart objects while accounting for the finite memory of sensors. RPL (Routing Protocol for Low-Power and Lossy Networks) is one of the developed solutions; it is a routing protocol designed for wireless networks that are low power and often prone to packet loss. It is a distance vector-based protocol that supports both multi-hop many-to-one and one-to-one communications. It typically operates over IEEE 802.15.4 channels (Winter et al. 2012).

3.3 Application Layer: The uppermost layer is user-controlled. The application layer manages consumer-related business analytics and business intelligence standards to enhance the country's socioeconomic outlook.

IoT architecture guides the development of IoT applications, such as:

- Smart Agriculture
- Smart transportation
- Automated supply chain. Regarding the Fourth Industrial Revolution

Big data analytics is the term used to describe the comprehensive examination of the vast quantity of important data that IoT devices at the physical layer have acquired. These data have a large volume, rapid generating speed, and several forms (Ducange, Pecori, and Mezzina 2018). To get actionable insights from this data, big data analytical techniques must be included into the entire IoT architecture. Machine learning algorithms may be quite helpful in extracting value and turning this large data into actionable information.

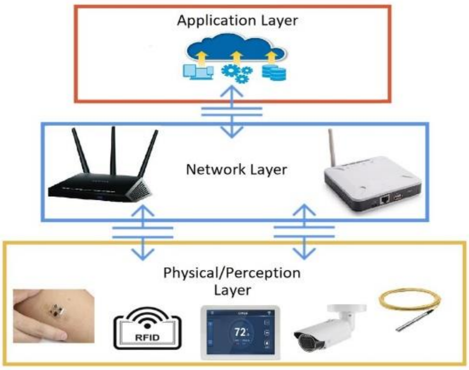

Figure1. The three-layered IOT security architectural framework (Azumah et al. 2021)

D. Literature Review

4.1 IoT Threat

The Internet of Things (IoT) is a collection of diverse sensing systems that are connected to one another over a local area network (LAN) (Hussain et al. 2020). Because end devices have access to more capabilities than conventional networks do, the hazards associated with the Internet of Things are different (Jing et al. 2014). The conventional Internet uses sophisticated computers and servers with plenty of resources, whereas the IoT uses basic hardware with limited memory and computational capacity. Real-world IoT devices cannot use multifactor authentication and dynamic protocols like normal networks. IoT wireless technologies like ZigBee and LoRa are less secure than conventional networks. A lack of a consistent operating system and functionality in IoT applications has led to different data contents and formats, making a unified security procedure difficult (Makhdoom et al. 2018). These weaknesses generate IoT security and privacy issues. Attacks increase with network growth. IoT networks are more susceptible than office or enterprise networks because they lack firewalls. Multi-vendor IoT systems that share data sometimes use a variety of wavelengths and protocols from various vendors. Connecting such devices is complex, requiring a trusted third party as a bridge (Brass et al. 2018). Many publications also question how billions of smart gadgets get app upgrades (Fernández-Caramés and Fraga-Lamas 2018), (Lee and Lee 2017). Small computer resources limit an IoT device's capacity to handle sophisticated threats. Lastly, IoT flaws might be crucial or pervasive. Although IoT vulnerabilities like battery depletion attacks, lack standards, and insufficient confidence are unique, internet-inherited weaknesses may be generic. Many IoT dangers have been found and classed (Mishra et al. 2018), (Butun, Österberg, and Song 2019),(Xiao et al. 2018). We discuss the issues that have been raised most often about the Internet of Things in the last ten years and attempt to group them according to privacy and security concerns. Basic concepts like privacy and security may improve network availability (Brewczyńska, Dunn, and Elijahu 2019),(Yuen 2019). Data on the internet of things may take many different forms, such as a user's identifying information, a command sent to a vehicle via a key fob, or a visual conversation between two individuals. Unauthorized disclosure of data may result in a breach of data availability, integrity, or security. A danger is considered a privacy threat if it jeopardizes confidentiality. Security threats put network stability and data confidentiality at risk (Bharati and Podder 2022). The several kinds of threats are crucial, as listed below:

4.1.1. Privacy threats

- Two forms of man-in-the-middle attacks exist: passive and active.
- Data privacy with MiTM attacks—passive and active.

4.1.2 Security threats

- MalwareOne of the most common attacks involves injecting and executing malicious code into IoT devices by exploiting vulnerabilities.
- Man-in-the-Middle. Early cyber risks included man-in-the-middle (MiTM) attacks (Bharati and Podder 2022). Impersonation and spoofing are examples of MiTM attacks.

• DDOS/DOS: Through public nodes, attackers attempt to use users' internet resources and bandwidth.

4.1.3. Other threats to privacy and security

• One kind of danger that is often impossible for a cyberattack to occur is physical harm or devastation.

• Cyber threat is classified as active threats, and passive threats.

(S M Jagannath et al. 2023) The many dangers that might arise in Internet of Things systems are shown in Figure 2.

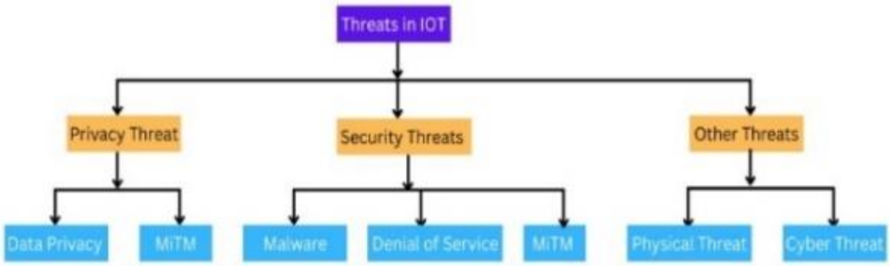

Figure 2. Kinds of threats in IOT

4.2 Deep Learning

DL uses multiple layers of Artificial Neural Networks (ANNs) to learn hierarchical representations in deep structures. DL architectures have several processing layers. Based on input layer data, each layer might respond non-linearly. The human brain's and neurons' signal processing methods are mimicked in DL's functioning. Compared to other conventional machine learning techniques, deep learning architectures have garnered more attention in the last several years. These methods are regarded as restricted subsets of shallow-structured learning architectures (DL). Figure 4 displays the Google trends search trend of five major machine learning algorithms, with DL rising in popularity. The notion of deep belief networks was developed by G. Hinton et al. in 2006, kicking off the DNN movement (Hinton and Salakhutdinov 2006). Subsequently, the technology's cutting-edge capabilities have been noted in several AI domains, such as picture identification, image recovery, information retrieval and search engines, and natural language processing. ANNs have been the foundation for the development of DL approaches. Neural Networks with Feed-forwarding (FNNs) (Svozil, Kvasnicka, and Pospichal 1997)(a.k.a Multilayer Perceptrons - MLPs) have been used to train systems for decades, but adding layers makes them harder to learn (Schmidhuber 2015). Another cause of overfitted models was small training data. Back then, computing resources limited the construction of efficient deeper FNNs. Recent technology improvements, especially GPUs and hardware accelerators, have addressed these processing restrictions. In addition to hardware and structural breakthroughs, DL approaches have benefitted from successful deep network training algorithms, such as:

• Utilizing Rectified Linear Units (ReLUs) as activation function (Glorot, Bordes, and Bengio 2011),

• Introducing dropout methods (Hinton et al. 2012),

- Random initialization for the weights of the network (Sutskever et al. 2013),
- Addressing the degradation of training accuracy by residual learning networks (He et al. 2016),
- Improving Long Short-Term Memory networks to solve vanishing and ballooning gradient problems (Hochreiter and Schmidhuber 1997), (Mikolov et al. 2014).

One benefit of DL architectures over regular ANNs is their ability to extract latent characteristics from unprocessed data (LeCun et al. 2015). Based on the preceding layer's results, each layer trains features. Since they collect and recombine information from preceding layers, the innermost layers may detect more complex features. This is featuring hierarchy. For example, a face recognition model receives portrait picture data as vectors of pixels in its input layer. The first hidden layer recognizes lines and edges, the second identifies facial components like noses, eyes, etc., and the third integrates all the prior characteristics to form a face. DL models' purported gains are based on empirical assessments, and there is no analytical basis for why they beat shallower methods. The number of hidden layers does not distinguish deep from shallow networks. Deep models include two or more hidden layers and use complex training techniques. Recurrent neural networks with one hidden layer are deep because their units contain a cycle that can be unrolled to a deep network (Mohammadi et al. 2018) .

4.3 Deep Learning Techniques

Stakeholders must understand the IoT and big data's core concepts, promise, and difficulties. IoT is a key generator and a target for Big Data research to improve IoT operations and services (Al-Fuqaha et al. 2015). IoT Big Data Research also shows its social benefit. IoT data differs from big data. We must study IoT data qualities (Chen et al. 2014) How they differ from typical big data for IoT data analytics. This article discusses the benefits of DL over standard ML approaches in IoT applications (Ma et al. 2019),(Rodrigues et al. 2022). DL can generalize the dynamic relationship of large raw data in IoT applications better than ML. DL models perform better in big data because their depths and architectures, including convolutional architectures, affect their ability to process data. Common learning models can easily be overwhelmed by a flood of data. Deep learning can automatically discover successful characteristics from raw data without manual implementations. DL models are more sentient than previous ML methods in recent years. Google trends reveal that DL is becoming more popular among ML techniques like random forest, k-means, SVM, and decision tree (Figure 3). Figure 4 demonstrates that CNN became the most used DL technique according to Google trends.

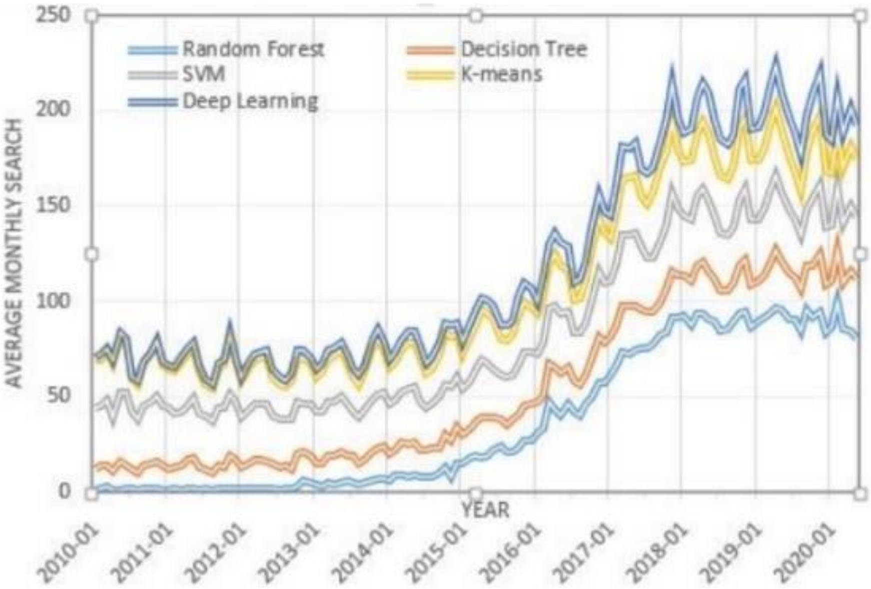

Figure 3. Recent Google trends indicate increased interest in DL

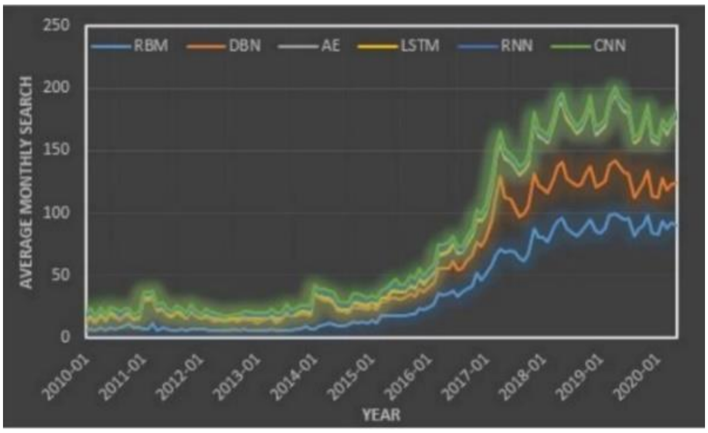

Figure 4. Recent Google trends reflect increasing CNN interest.

Deep learning is a new multilayer neural network method. It transformed machine learning, advancing artificial intelligence and human–computer interaction. They tested CNN and DBN on MNIST and real-world handwritten character databases and found 99.28% and 98.12% accuracy (K Lakshmanna et al. 2022). In spite of its complexity and variety of user data, researchers (Khosravy et al. 2022) We suppose the MIA in a semi-white box situation where system model structures and parameters are known but user data is not, and show that it is a severe concern even for a deep-learning-based face recognition system. Power plants' lifespan effects on GEP are examined in this article (Dehghani et al. 2021). Deep learning is also used for time series forecasting. DL has sophisticated knowledge-boosting algorithms that can analyze lots of unstructured data (Zantalis et al. 2019). These methods are suited for huge data management and computer-intensive tasks including picture pattern recognition, speech recognition, and analysis. DL requires significant computer capabilities and takes time in the model training cycle, which has been a major hurdle. DL activities that demand more CPU power are often done with efficient GPUs. In the age of big data, DL is a prominent data processing and modeling method (Ma et al. 2019). DL uses a limited number of layers with certain properties. Before applying DL, functionality is automatically calculated and feature computation and extraction are not needed. DL also presents several network architectures. The goal of the authors (Hussain and Park 2021),(Hussain et al. 2022) EEG characteristics will be quantified to better understand task-induced neurological deficits caused by stroke and to analyze biomarkers to identify ischemic stroke patients from healthy people. In training and predicting, DL models often outperform ML techniques in two ways (Mohammadi et al. 2018). They first reduce human training and then delete elements that may be unclear to humans (LeCun et al. 2015). DL approaches boost accuracy. DL, In the next subsections, we will outline the major deep neural network types uncovered in our systematic review (Kuruva Lakshmanna et al. 2022).

4.3.1 Unsupervised Deep Neural Networks

Unlabeled data collecting is simple. To handle enormous unlabeled data, unsupervised learning must be used with traditional approaches. The training may use stacked RBMs or autoencoders for stable initialization, back propagation, and global fine-tuning.

4.3.1.1 Restricted Boltzmann Machines

Restricted Boltzmann machines (RBMs) (Fischer and Igel 2012) are stochastic neural network-like probabilistic graphical models. RBMs express output stochastically with m visible units for observable data and n hidden units for collections between observed variables. Two-level RBM with m visible and n hidden variables is shown in Fig. 5. Successful dimensionality reduction and collaborative filtering by RBMs (Salakhutdinov, Mnih, and Hinton 2007). A Deep Belief Network (DBN) forms a deep learning model by stacking RBMs (Hinton, Osindero, and Teh 2006), A greedy learning algorithm trains it layer-by-layer, and the contrastive divergence (CD) approach updates the weights. Neural networks trap in non-convex function local optima, resulting in poor performance (DE 1986). DBN builds models using unsupervised pre-training and supervised fine-tuning. The former learns data distributions using unlabeled data, while the latter fine-tunes with labeled data to find the best answer (Hinton and Salakhutdinov 2006).

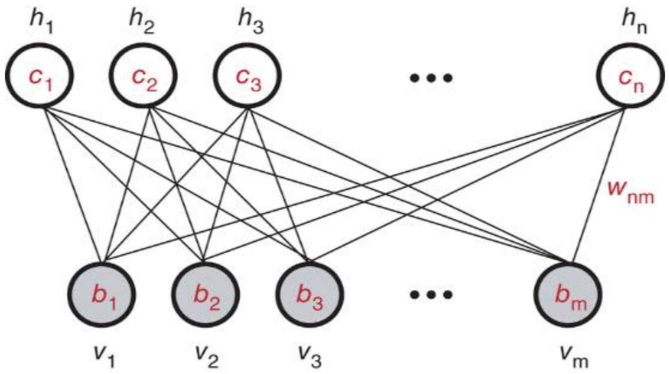

Figure 5. An RBM with n hidden variables and m displayed variables.

4.3.1.2 Autoencoder

An autoencoder (Anon 2020) A neural network that copies its input to its output. In contrast to RBMs, autoencoders have three layers: input, hidden, and output. The buried layer reconstructs the input from its code. The network's encoder f retrieves input dependencies, and its decoder g reconstructs them. Minimizing input-output error trains autoencoder. Fig. 6 illustrates a simple autoencoder design and example. A layer-by-layer stack of autoencoders may create a deep model, like RBMs. The hidden layer of a well-trained autoencoder is supplied as the input layer of another, creating a multilayer model. Sparse autoencoders exist (Lee et al. 2006), denoising autoencoder (Vincent et al. 2008), and contractive autoencoder.

4.3.2 Supervised deep neural networks

Supervised learning builds the system model using a labeled training set. The model learns input-output-system parameter relationships. The back propagation technique dominates supervised learning (DE 1986).

4.3.2.1 Convolutional Neural Networks (CNNs)

CNN is a grid-like neural network for data processing (Anon 2020).

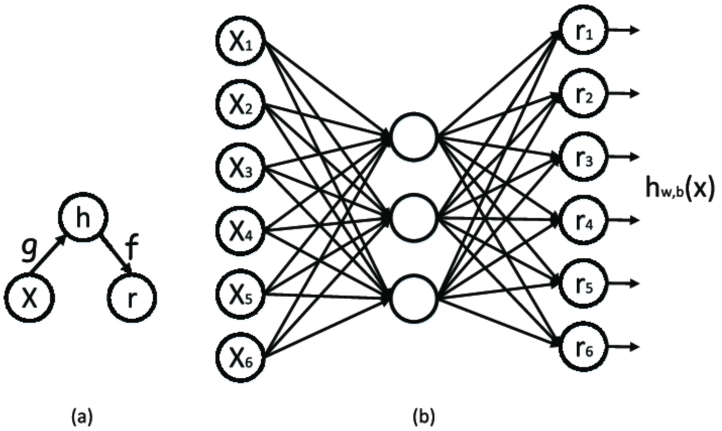

Figure.6 (a) A generic auto encoder’s structure, and (b) a particular auto encoder structure diagram which includes 6 input data

Receptive Field, a notion from cat visual brain research, influenced CNNs (Hubel and Wiesel 1968). Convolution uses sparse interactions, parameter sharing, and equivariant representations to enhance machine learning. An optional fully connected layer for classification or prediction follows one convolutional and pooling layer in the CNN design. Instead of classic neural networks, CNNs effectively reduce net parameters and gradient diffusion issue, allowing us to train a deep model with more than 10 layers. For example, AlexNet (Krizhevsky, Sutskever, and Hinton 2012) contains 9 layers, VGGNet (Simonyan and Zisserman 2014) contains 11-19 layers, InceptionNet (Szegedy et al. 2015) from Google contains more than 22 layers, and ResNet (He et al. 2016) from Microsoft even contains 152 layers. Fig. 7 shows a general architecture of traditional CNNs called LeNet (LeCun et al. 1995).

4.3.2.2 Recurrent Neural Networks (RNNs)

Serial data processing neural networks are RNNs. RNNs can scale longer sequences than non-specialized networks. Many RNNs use equation or a similar equation h (t) = f (h t−1, x (t); θ) to define the values of their hidden units, illustrated in Fig. 8 (Goodfellow, Bengio, and Courville 2016). The network topology shows that RNNs may recall earlier information and impact future node output. Due to gradient dispersion and long-term dependencies, RNNs can only look back a few steps. To tackle these challenges, innovative methods like LSTM (Long Short-Term Memory) (Hochreiter and Schmidhuber 1997) and GRU (Gated Recurrent Unit) (Chung et al. 2014) are presented to model the hidden state to determine what to maintain in prior and current memory. These variations effectively capture long-term dependencies and improve language comprehension. RNN focuses on temporally continuous data connections, unlike CNN. Thus, RNN is primarily used in NLP (Yu, Lee, and Le 2017)(Cho et al. 2014)(Ma et al. 2019).

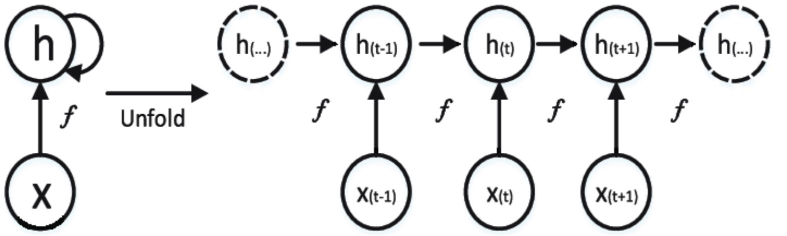

Figure 7. The architecture of Le Net 5. Each of these planes indicate a feature map. Kernels-little white boxes-are convolutional neural network keys. The graphic shows that convolutional layers emphasize local associations more than complete connection layers.

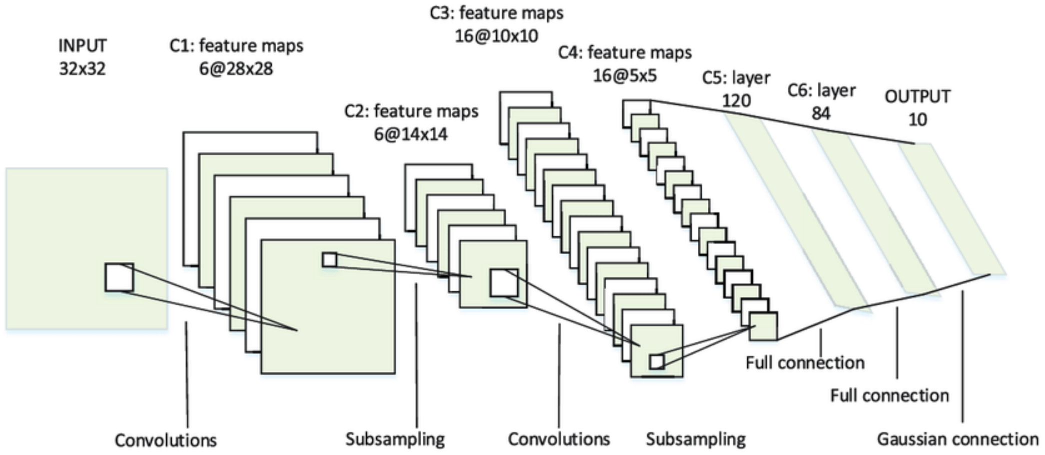

Figure 8. A universal unfolding recurrent neural network structure without output.

4.3.2.3 Long Short-Term Memory (LSTM)

LSTMs extend RNNs. Different LSTM versions have been suggested, although most follow the basic network architecture (Hochreiter and Schmidhuber 1997). Each gate in LSTM computes a value between 0 and 1 depending on input. In addition to a feedback loop to retain information, LSTM neurons (memory cells) include multiplicative forget, read, and write gates. These gates restrict memory cell access and protect them from irrelevant inputs. Neurons write data to themselves while the forget gate is activated. When the forget gate is switched off with 0, the neuron forgets its last content. With the write gate set to 1, other neurons may write to that neuron. With the read gate set to 1, linked neurons may read neuron content. Figure 9 depicts this structure. LSTMs use forget gates to actively manage cell states and prevent degradation, unlike RNNs. The gates may activate using sigmoid or tanh. Other models utilizing similar activation functions have disappearing gradients during backpropagation during training. Knowing what data to recall in LSTMs,

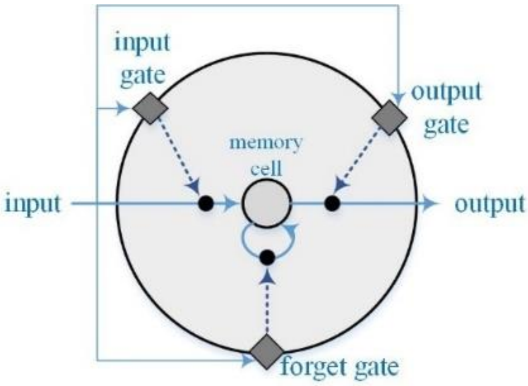

Figure 9. Structure of an LSTM memory cell. Data flow is depicted by solid arrow lines, whereas gate signals are shown by dashed arrow lines.

time does not affect memory cell calculations. BPTT is a typical error-reducing network training approach. When data is time-dependent, LSTM models outperform RNN models (Chung et al. 2014). IoT applications including human activity detection, online program educational performance prediction, and environmental monitoring-based hazard prediction exhibit this lengthy dependence lag.

4.3.3 Hybrid deep neural networks

The first DNN in this category is a GAN (Mohammadi et al. 2018), which trains generative and discriminative models simultaneously using an adversarial method. The former learns the input data distribution and creates data samples, while the latter evaluates a sample's authenticity by predicting that it originates from the training dataset rather than the generating samples. Generating a sample from random noise increases the likelihood of misleading the discriminative model in categorizing it. However, the discriminative model, given actual data samples and random noise samples, classifies samples from both sources. After measuring their performance, both models are repeatedly modified such that the discriminative model's output helps the generative model enhance the next iteration's samples (Mohammadi et al. 2018). Many benefits of a GAN include:

- It can handle zero-day assaults and give algorithms with new samples since it can learn fresh circumstances;
- appropriate for semi-supervised training;
- it creates samples faster than a visible DBN. GANs create a sample with one pass into the model, whereas RBMs repeat a Markov chain an unknown number of times (Salimans et al. 2016).

However, GANs have two drawbacks: (i) the training phase is unstable and (ii) the generative model struggles to generate discrete data (Goodfellow et al.

2014). EDLNs are another hybrid DNN. Together, DL generative, discriminative, and hybrid models perform better than individually. EDLNs are used for complicated jobs because of their uncertainty and high-dimensional characteristics. The ensemble may include homogeneous and heterogeneous DL classifiers, improving performance and generalization (Kuncheva 2014). EDLNs have been successful in many areas, such as detecting human actions, but their direct application to IoT security needs light classifiers that can function in a distributed setting.

4.3.4 Deep reinforcement learning

Deep Q-learning Networks are a prime example. These combine CNNs with the Q-learning algorithm, utilized for reinforcement learning in legacy machine learning. The neural network approximates the Q-function by receiving status as an input and producing the Qvalues of all feasible actions as outputs (Mnih et al. 2015). The neural network's maximum output, whose loss function is usually the mean squared error of the predicted Q-value and the target Q-value, determines the next action, making this a reinforcement learning regression problem with an unknown target or actual value. To converge, the network back-propagates its gradient. Non-stationary or unsteady targets are a DQN downside. DQNs' target changes in each iteration, but standard deep learning's target variable stays the same, making training stable. DQNs may also use two neural networks in the same structure: one for real-time updates and the other for synchronous parameter updates per time interval, enhancing algorithm convergence.

4.3.4 Applications of IoT

IoT applications are categorized by their core characteristics. For IoT data analysis to work, several issues must be considered. Figure 10 shows several IoT uses. The following categories describe IoT applications:

1. Smart Home Smart house is likely the first IoT application. According to IoT data, over 70,000 individuals seek for a "smart home" monthly. Big firms invest IoT startups for smart home initiatives. Smart home products including washing machines, refrigerators, lamps, fans, TVs, and smart doors may interact online with approved users to improve monitoring, management, and energy efficiency.

2. Smart City: Smart cities include various characteristics including the optimum traffic system idea. This category focuses on cities. Most cities have the same issues. Sometimes they differ by city. Many cities face global issues including clean drinking water, air pollution, and urban crowding. City IoT applications include water, trash, security, temperature monitoring, traffic, and more. Smart city transportation reduces noise, pollution, accidents, parking, street light issues, and public transit.

3. Health care: Modern medical instruments lack real-world expertise. It focuses on regulated settings, medical examination volunteers, and surviving data. Through study, real-time field data, and testing, IoT unlocks a wealth of usable data. New medical solutions employing IoT aim to enhance patient health (Lakshmanna, Khare, and Khare 2016),(Lakshmanna and Khare 2016). Without physicians or medical staff, sensors can monitor a wound's, blood pressure, heart rate, sugar, oxygen, body temperature, etc. In the article (Hussain, Young, and Park 2021), physiological signals are rapid and sensitive to neurological changes

generated by cognitive load from varied driving situations and are used to analyze the link between neurological outcomes and driving settings.

4. Security: Smart cameras from IoT can boost global security. Real-time digital image recognition helps smart security systems spot crooks and avert harm. IoT security is the greatest issue.

5. Smart Retail: One of the major IoT applications. Tracking items on the road or getting suppliers to provide inventory data has been available for years. However, it is restricted. Intelligent GPS and RFID technology allow product tracking from output to storing easier and save time and money. Retailers use IoT for location monitoring, inventory management, equipment maintenance, mall traffic analysis, etc.

6. Agriculture: Many academics have studied this developing IoT use (Gupta et al. 2020),(Garg, Khan, and Alam 2020). Connected devices have spread to health and well-being, home automation, vehicle and logistics, intelligent cities, security, retail, and industrial IoT. Since agricultural activities are remote and the IoT can monitor various resources, farmers may adjust their methods. The biggest issue is converting farmers to smart farming. Checking soil quality, weather, cost management, waste, crop management, etc. might help them.

7. Wearables: Today, everyone may wear wearables to monitor heart rate, sugar, oxygen, blood pressure, temperature, sleeping condition, walk distance, etc. Wearable gear is great for IoT applications and one of the first sectors to utilize it.

8. Industrial Automation: In addition to remote access and control, industrial IoT networking allows data extraction, processing, exchange, and analysis by multiple data sources. This may boost productivity and performance greatly. Cost effectiveness and quick development define IoT solutions. To improve cost and customer service, IoT Applications may quickly re-engineer devices and packaging with automation. Products flow monitoring, digitalization, quality control, safety and security, packaging optimization, logistics, and supply chain optimization is some uses.

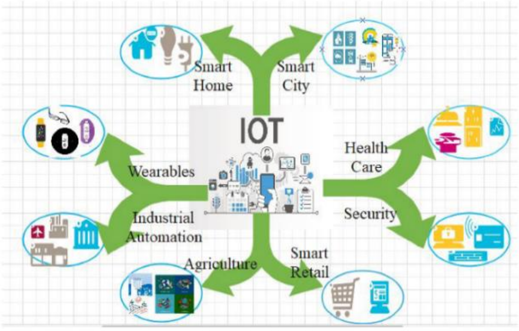

Figure 10. Applications of IoT

E. Conclusion

In this paper, DL and IoT approaches are reviewed in smart house, smart city, smart transit, energy, localization, health sector, security, agriculture, etc. In recent years, academics and businesses have focused on DL and IoT, which have improved our lives, cities, and the planet. DL resources assist several IoT applications. Large-scale data analysis challenges are solved well by DL models.

We used enormous datasets created at rising rates owing to the newest IoT frameworks and open-source libraries to train and develop the DL model. The literature recommended training models using scattered IoT devices rather than cluster-like infrastructure. Distributed solution must handle data privacy, IO operation time, and high complexity. The closing debate illuminated numerous outstanding concerns on the subject we chose, demonstrating the necessity for further research to make DL a permanent and mature solution to IoT security. We want to investigate more effective data drop and reconstruction techniques in the future in order to increase classification accuracy on both clean samples and AEs. The throughput of the network may be further decreased with a higher drop ratio and improved restoration techniques. We will also investigate more sophisticated protection strategies against more sophisticated assaults, such as adaptive adversarial attacks, for a IoT systems.

F. References

[1] Abomhara, Mohamed, and Geir M. Køien. 2015. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." Journal of Cyber Security and Mobility 65–88.

[2] Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials 17(4):2347–76.

[3] Al-Garadi, Mohammed Ali, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. 2020. "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security." IEEE Communications Surveys & Tutorials 22(3):1646–85.

[4] Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. "Internet of Things Security: A Survey." Journal of Network and Computer Applications 88:10–28.

[5] Alkahtani, Hasan, and Theyazn H. H. Aldhyani. 2021. "Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms." Complexity 2021. doi: 10.1155/2021/5579851.

[6] Almutairi, Ashwaq Fahhad, and Asma Abdulghani Alshargabi. 2022. "Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment." 2022 2nd International Conference on Emerging Smart Technologies and Applications, ESmarTA 2022 1–6. doi: 10.1109/eSmarTA56775.2022.9935467.

[7] Anon. 2020. Advances in Deep Learning. Springer.

[8] Aversano, Lerina, Mario Luca Bernardi, Marta Cimitile, and Riccardo Pecori. 2021. "A Systematic Review on Deep Learning Approaches for IoT Security." Computer Science Review 40:100389. doi: 10.1016/j.cosrev.2021.100389.

[9] Azumah, Sylvia Worlali, Nelly Elsayed, Victor Adewopo, Zaghloul Saad Zaghloul, and Chengcheng Li. 2021. "A Deep Lstm Based Approach for Intrusion Detection Iot Devices Network in Smart Home." Pp. 836–41 in 2021 IEEE 7th World Forum on Internet of Things (WF-IoT).

[10] Bakhsh, Shahid Allah, Muhammad Almas Khan, Fawad Ahmed, Mohammed S. Alshehri, Hisham Ali, and Jawad Ahmad. 2023. “Enhancing IoT Network Security through Deep Learning-Powered Intrusion Detection System.” Internet of Things (Netherlands) 24(July):100936. doi: 10.1016/j.iot.2023.100936.

[11] Banaamah, Alaa Mohammed, and Iftikhar Ahmad. 2022. “Intrusion Detection in IoT Using Deep Learning.” Sensors 22(21). doi: 10.3390/s22218417.

[12] Bertino, Elisa, and Nayeem Islam. 2017. “Botnets and Internet of Things Security.” Computer 50(2):76–79.

[13] Bharati, Subrato, and Prajoy Podder. 2022. “Machine and Deep Learning for Iot Security and Privacy: Applications, Challenges, and Future Directions.” Security and Communication Networks 2022:1–41.

[14] Bharati, Subrato, Prajoy Podder, and M. Rubaiyat Hossain Mondal. 2020. “Hybrid Deep Learning for Detecting Lung Diseases from X-Ray Images.” Informatics in Medicine Unlocked 20:100391.

[15] Bonetto, Riccardo, Ilya Sychev, Oleksandr Zhdanenko, Abdelrahman Abdelkader, and Frank H. P. Fitzek. 2020. “Smart Grids for Smarter Cities.” Pp. 1–2 in 2020 IEEE 17th Annual Consumer Communications \& Networking Conference (CCNC).

[16] Brass, Irina, Leonie Tanczer, Madeline Carr, Miles Elsden, and Jason Blackstock. 2018. “Standardising a Moving Target: The Development and E volution of IoT Security Standards.”

[17] Brewczyńska, Magda, Suzanne Dunn, and Avihai Elijahu. 2019. “Data Privacy Laws Response to Ransomware Attacks: A Multi-Jurisdictional Analysis.” Regulating New Technologies in Uncertain Times 281–305.

[18] Butun, Ismail, Patrik Österberg, and Houbing Song. 2019. “Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures.” IEEE Communications Surveys \& Tutorials 22(1):616–44.

[19] Calabretta, Marco, Riccardo Pecori, Massimo Vecchio, and Luca Veltri. 2018. “MQTT-Auth: A Token-Based Solution to Endow MQTT with Authentication and Authorization Capabilities.” Journal of Communications Software and Systems 14(4):320–31.

[20] Calabretta, Marco, Riccardo Pecori, and Luca Veltri. 2018. “A Token-Based Protocol for Securing MQTT Communications.” Pp. 1–6 in 2018 26th International conference on software, telecommunications and computer networks (SoftCOM).

[21] Chen, Min, Shiwen Mao, Yin Zhang, Victor C. M. Leung, and others. 2014. Big Data: Related Technologies, Challenges and Future Prospects. Vol. 100. Springer.

[22] Cho, Kyunghyun, Bart Van Merriënboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. 2014. “Learning Phrase Representations Using RNN Encoder-Decoder for Statistical Machine Translation.” ArXiv Preprint ArXiv:1406.1078.

[23] Chung, Junyoung, Caglar Gulcehre, KyungHyun Cho, and Yoshua Bengio. 2014. “Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling.” ArXiv Preprint ArXiv:1412.3555.

[24] DE, RUMELHART. 1986. "Learning Representations by Back-Propagation Errors." Nature 323:533–36.

[25] Dehghani, Majid, Mohammad Taghipour, Saleh Sadeghi Gougheri, Amirhossein Nikoofard, Gevork B. Gharehpetian, and Mahdi Khosravy. 2021. "A Deep Learning-Based Approach for Generation Expansion Planning Considering Power Plants Lifetime." Energies 14(23):8035.

[26] Ducange, Pietro, Riccardo Pecori, and Paolo Mezzina. 2018. "A Glimpse on Big Data Analytics in the Framework of Marketing Strategies." Soft Computing 22(1):325–42.

[27] Elsayed, Nelly, Zag Elsayed, and Magdy Bayoumi. 2023. "IoT Botnet Detection Using an Economic Deep Learning Model." 2023 IEEE World AI IoT Congress, AIIoT 2023 (c):134–42. doi: 10.1109/AIIoT58121.2023.10174322.

[28] Fadlullah, Zubair Md, Fengxiao Tang, Bomin Mao, Nei Kato, Osamu Akashi, Takeru Inoue, and Kimihiro Mizutani. 2017. "State-of-the-Art Deep Learning: Evolving Machine Intelligence toward Tomorrow's Intelligent Network Traffic Control Systems." IEEE Communications Surveys \& Tutorials 19(4):2432–55.

[29] Fernández-Caramés, Tiago M., and Paula Fraga-Lamas. 2018. "A Review on the Use of Blockchain for the Internet of Things." Ieee Access 6:32979–1.

[30] Fischer, Asja, and Christian Igel. 2012. "An Introduction to Restricted Boltzmann Machines." Pp. 14–36 in Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications: 17th Iberoamerican Congress, CIARP 2012, Buenos Aires, Argentina, September 3-6, 2012. Proceedings 17.

[31] Garg, Disha, Samiya Khan, and Mansaf Alam. 2020. "Integrative Use of IoT and Deep Learning for Agricultural Applications." Pp. 521–31 in Proceedings of ICETIT 2019: Emerging Trends in Information Technology.

[32] Glorot, Xavier, Antoine Bordes, and Yoshua Bengio. 2011. "Deep Sparse Rectifier Neural Networks." Pp. 315–23 in Proceedings of the fourteenth international conference on artificial intelligence and statistics.

[33] Goodfellow, Ian, Yoshua Bengio, and Aaron Courville. 2016. Deep Learning. MIT press.

[34] Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. "Generative Adversarial Nets." Advances in Neural Information Processing Systems 27.

[35] Gupta, Neeraj, Mahdi Khosravy, Nilesh Patel, Nilanjan Dey, Saurabh Gupta, Hemant Darbari, and Rubén González Crespo. 2020. "Economic Data Analytic AI Technique on IoT Edge Devices for Health Monitoring of Agriculture Machines." Applied Intelligence 50:3990–4016.

[36] Hassaan Khalid, Muhammad, Hanan Sharif, Faisal Rehman, Muhammad Naeem Ullah, Shahbaz Shaukat, Hadia Maqsood, Chaudhry Nouman Ali, Ayaz Hussain, and Irfana Iftikhar. 2023. "A Brief Overview of Deep Learning Approaches for IoT Security." 2023 4th International Conference on Computing, Mathematics and Engineering Technologies: Sustainable Technologies for Socio-Economic Development, ICoMET 2023. doi: 10.1109/iCoMET57998.2023.10099306.

[37] He, Kaiming, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. 2016. "Deep Residual Learning for Image Recognition." Pp. 770–78 in Proceedings of the IEEE conference on computer vision and pattern recognition.

[38] Hinton, Geoffrey E., Simon Osindero, and Yee-Whye Teh. 2006. “A Fast Learning Algorithm for Deep Belief Nets.” Neural Computation 18(7):1527–54.

[39] Hinton, Geoffrey E., and Ruslan R. Salakhutdinov. 2006. “Reducing the Dimensionality of Data with Neural Networks.” Science 313(5786):504–7.

[40] Shavan Askar & Kurdistan Ali & Tarik A. Rashid, 2021. "Fog Computing Based IoT System: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 183-196.

[41] Shavan Askar & Kosrat Dlshad Ahmed & Shahab Wahhab Kareem, 2021. "Deep learning Utilization in SDN Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 174-182.

[42] Ibrahim Shamal Abdulkhaleq & Shavan Askar, 2021. "Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 71-82.

[43] F. E. F. Samann, S. R. M. Zeebaree, and S. Askar, “IoT Provisioning QoS based on Cloud and Fog Computing”, JASTT, vol. 2, no. 01, pp. 29 - 40, Mar. 2021.

[44] Hinton, Geoffrey E., Nitish Srivastava, Alex Krizhevsky, Ilya Sutskever, and Ruslan R. Salakhutdinov. 2012. “Improving Neural Networks by Preventing Co-Adaptation of Feature Detectors.” ArXiv Preprint ArXiv:1207.0580.

[45] Hochreiter, Sepp, and Jürgen Schmidhuber. 1997. “Long Short-Term Memory.” Neural Computation 9(8):1735–80.

[46] Hubel, David H., and Torsten N. Wiesel. 1968. “Receptive Fields and Functional Architecture of Monkey Striate Cortex.” The Journal of Physiology 195(1):215–43.

[47] Hussain, Fatima, Syed Ali Hassan, Rasheed Hussain, and Ekram Hossain. 2020. “Machine Learning for Resource Management in Cellular and IoT Networks: Potentials, Current Solutions, and Open Challenges.” IEEE Communications Surveys \& Tutorials 22(2):1251–75.

[48] Hussain, Iqram, Md Azam Hossain, Rafsan Jany, Md Abdul Bari, Musfik Uddin, Abu Raihan Mostafa Kamal, Yunseo Ku, and Jik-Soo Kim. 2022. “Quantitative Evaluation of EEG-Biomarkers for Prediction of Sleep Stages.” Sensors 22(8):3079.

[49] Hussain, Iqram, and Se-Jin Park. 2021. “Quantitative Evaluation of Task-Induced Neurological Outcome after Stroke.” Brain Sciences 11(7):900.

[50] Hussain, Iqram, Seo Young, and Se-Jin Park. 2021. “Driving-Induced Neurological Biomarkers in an Advanced Driver-Assistance System.” Sensors 21(21):6985.

[51] Jagannath, S M, R. B. Mohite, M. K. Gupta, and O. S. Lamba. 2023. “Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems Indian Journal of Science and Technology 16 (9): 640-647.”

[52] Jagannath, Salunkhe Madhav, Rajendra B. Mohite, Mukesh Kumar Gupta, and Onkar S. Lamba. 2023. “Implementation of Machine Learning and Deep Learning for Securing the Devices in IOT Systems.” Indian Journal Of Science And Technology 16(9):640–47. doi: 10.17485/ijst/v16i9.99.

[53] Jing, Qi, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. 2014. “Security of the Internet of Things: Perspectives and Challenges.” Wireless Networks 20:2481–2501.

[54] Jose, Jinsi, and Deepa V. Jose. 2021. "Performance Analysis of Deep Learning Algorithms for Intrusion Detection in IoT." ICCISc 2021 - 2021 International Conference on Communication, Control and Information Sciences, Proceedings 1:1–6. doi: 10.1109/ICCISc52257.2021.9484979.

[55] Karne, RadhaKrishna, S. Mounika, KarthikKumar V, and Dr. Nookala Venu. 2022. "Applications of IoT on Intrusion Detection System with Deep Learning Analysis." (August).

[56] Khosravy, Mahdi, Kazuaki Nakamura, Yuki Hirose, Naoko Nitta, and Noboru Babaguchi. 2022. "Model Inversion Attack by Integration of Deep Generative Models: Privacy-Sensitive Face Generation from a Face Recognition System." IEEE Transactions on Information Forensics and Security 17:357–72.

[57] Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. "DDoS in the IoT: Mirai and Other Botnets." Computer 50(7):80–84.

[58] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. 2012. "Imagenet Classification with Deep Convolutional Neural Networks." Advances in Neural Information Processing Systems 25.

[59] Kuncheva, Ludmila I. 2014. Combining Pattern Classifiers: Methods and Algorithms. John Wiley \& Sons.

[60] Lakshmanna, K, R. Kaluri, G. Nagaraja, Z. S. Alzamil, D. S. Rajput, A. A. Khan, M. A. Haq, and A. Alhussen. 2022. "A Review on Deep Learning Techniques for IoT Data. Electronics 2022, 11, 1604."

[61] Lakshmanna, Kuruva, Rajesh Kaluri, Nagaraja Gundluru, Zamil S. Alzamil, Dharmendra Singh Rajput, Arfat Ahmad Khan, Mohd Anul Haq, and Ahmed Alhussen. 2022. "A Review on Deep Learning Techniques for IoT Data." Electronics (Switzerland) 11(10). doi: 10.3390/electronics11101604.

[62] Lakshmanna, Kuruva, and Neelu Khare. 2016. "FDSMO: Frequent DNA Sequence Mining Using FBSB and Optimization." International Journal of Intelligent Engineering and Systems 9(4):157–66.

[63] Lakshmanna, Kuruva, Neelu Khare, and N Khare. 2016. "Constraint-Based Measures for DNA Sequence Mining Using Group Search Optimization Algorithm." International Journal of Intelligent Engineering and Systems 9(3):91–100.

[64] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. 2015. "Deep Learning." Nature 521(7553):436–44.

[65] LeCun, Yann, Lawrence D. Jackel, Léon Bottou, Corinna Cortes, John S. Denker, Harris Drucker, Isabelle Guyon, Urs A. Muller, Eduard Sackinger, Patrice Simard, and others. 1995. "Learning Algorithms for Classification: A Comparison on Handwritten Digit Recognition." Neural Networks: The Statistical Mechanics Perspective 261(276):2.

[66] Lee, Boohyung, and Jong-Hyouk Lee. 2017. "Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment." The Journal of Supercomputing 73:1152–67.

[67] Lee, Honglak, Alexis Battle, Rajat Raina, and Andrew Ng. 2006. "Efficient Sparse Coding Algorithms." Advances in Neural Information Processing Systems 19.

[68] Lee, In. 2020. "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management." Future Internet 12(9):157.

[69] Li, He, Kaoru Ota, and Mianxiong Dong. 2018. “Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing.” IEEE Network 32(1):96–101.

[70] Li, Yuxi, Yue Zuo, Houbing Song, and Zhihan Lv. 2021. “Deep Learning in Security of Internet of Things.” IEEE Internet of Things Journal 9(22):22133–46.

[71] Liang, Fan, Wei Yu, Xing Liu, David Griffith, and Nada Golmie. 2020. “Toward Edge-Based Deep Learning in Industrial Internet of Things.” IEEE Internet of Things Journal 7(5):4329–41.

[72] Ma, Xiaoqiang, Tai Yao, Menglan Hu, Yan Dong, Wei Liu, Fangxin Wang, and Jiangchuan Liu. 2019. “A Survey on Deep Learning Empowered IoT Applications.” IEEE Access 7:181721–32.

[73] Makhdoom, Imran, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, and Wei Ni. 2018. “Anatomy of Threats to the Internet of Things.” IEEE Communications Surveys \& Tutorials 21(2):1636–75.

[74] Shavan Askar & Zhala Jameel Hamad & Shahab Wahhab Kareem, 2021. "Deep Learning and Fog Computing: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 197-208.

[75] Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. 2013. Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. Vol. 180. McKinsey Global Institute San Francisco, CA.

[76] Mikolov, Tomas, Armand Joulin, Sumit Chopra, Michael Mathieu, and Marc’Aurelio Ranzato. 2014. “Learning Longer Memory in Recurrent Neural Networks.” ArXiv Preprint ArXiv:1412.7753.

[77] Mishra, Preeti, Vijay Varadharajan, Uday Tupakula, and Emmanuel S. Pilli. 2018. “A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection.” IEEE Communications Surveys \& Tutorials 21(1):686–728.

[78] Chnar Mustaf Mohammed & Shavan Askar, 2021. "Machine Learning for IoT HealthCare Applications: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 42-51.

[79] Zhala Jameel Hamad & Shavan Askar, 2021. "Machine Learning Powered IoT for Smart Applications," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 92-100.

[80] Mnih, Volodymyr, Koray Kavukcuoglu, David Silver, Andrei A. Rusu, Joel Veness, Marc G. Bellemare, Alex Graves, Martin Riedmiller, Andreas K. Fidjeland, Georg Ostrovski, and others. 2015. “Human-Level Control through Deep Reinforcement Learning.” Nature 518(7540):529–33.

[81] Mohammadi, Mehdi, Ala Al-Fuqaha, Sameh Sorour, and Mohsen Guizani. 2018. “Deep Learning for IoT Big Data and Streaming Analytics: A Survey.” IEEE Communications Surveys and Tutorials 20(4):2923–60. doi: 10.1109/COMST.2018.2844341.

[82] Pecori, Riccardo. 2012. “A PKI-Free Key Agreement Protocol for P2P VoIP Applications.” Pp. 6748–52 in 2012 IEEE International Conference on Communications (ICC).

[83] Saman M. Omer, Kayhan Z. Ghafoor, Shavan K. Askar, "An Intelligent System for Cucumber Leaf Disease Diagnosis Based on the Tuned Convolutional Neural Network Algorithm" Journal of Mobile Information systems, Volume 2022.

[84] Shavan Askar & Chnar Mustaf Mohammed & Shahab Wahhab Kareem, 2021. "Deep Learning in IoT systems: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 131-147.

[85] Pecori, Riccardo. 2019. "Augmenting Quality of Experience in Distance Learning Using Fog Computing." IEEE Internet Computing 23(5):49–58.

[86] Pecori, Riccardo, Pietro Ducange, and Francesco Marcelloni. 2019. "Incremental Learning of Fuzzy Decision Trees for Streaming Data Classification." Pp. 748–55 in 11th Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019).

[87] Pecori, Riccardo, Amin Tayebi, Armando Vannucci, and Luca Veltri. 2020. "IoT Attack Detection with Deep Learning Analysis." Pp. 1–8 in 2020 International Joint Conference on Neural Networks (IJCNN).

[88] Perrone, Giovanni, Massimo Vecchio, Riccardo Pecori, Raffaele Giaffreda, and others. 2017. "The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-Attack Carried Out through an Army of IoT Devices." Pp. 246–53 in IoTBDS.

[89] Rahman, Md Abdur, and M. Shamim Hossain. 2021. "An Internet-of-Medical-Things-Enabled Edge Computing Framework for Tackling COVID-19." IEEE Internet of Things Journal 8(21):15847–54.

[90] Shavan Askar & Zhwan Mohammed Khalid & Tarik A. Rashid, 2021. "Blockchain For Securing IoT Devices: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 209-224.

[91] Rodrigues, Anisha P., Roshan Fernandes, Adarsh Shetty, Kuruva Lakshmanna, R. Mahammad Shafi, and others. 2022. "Real-Time Twitter Spam Detection and Sentiment Analysis Using Machine Learning and Deep Learning Techniques." Computational Intelligence and Neuroscience 2022.

[92] Salakhutdinov, Ruslan, Andriy Mnih, and Geoffrey Hinton. 2007. "Restricted Boltzmann Machines for Collaborative Filtering." Pp. 791–98 in Proceedings of the 24th international conference on Machine learning.

[93] Salimans, Tim, Ian Goodfellow, Wojciech Zaremba, Vicki Cheung, Alec Radford, and Xi Chen. 2016. "Improved Techniques for Training Gans." Advances in Neural Information Processing Systems 29.

[94] Schmidhuber, Jürgen. 2015. "Deep Learning in Neural Networks: An Overview." Neural Networks 61:85–117.

[95] Sethi, Pallavi, Smruti R. Sarangi, and others. 2017. "Internet of Things: Architectures, Protocols, and Applications." Journal of Electrical and Computer Engineering 2017.

[96] Shadroo, Shabnam, Amir Masoud Rahmani, and Ali Rezaee. 2021. "The Two-Phase Scheduling Based on Deep Learning in the Internet of Things." Computer Networks 185:107684.

[97] Simonyan, Karen, and Andrew Zisserman. 2014. "Very Deep Convolutional Networks for Large-Scale Image Recognition." ArXiv Preprint ArXiv:1409.1556.

[98] Sutskever, Ilya, James Martens, George Dahl, and Geoffrey Hinton. 2013. “On the Importance of Initialization and Momentum in Deep Learning.” Pp. 1139–47 in International conference on machine learning.

[99] Diana Hayder Hussein; Shavan Askar, “Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment”, IEEE Access, Volume 11, 2023.

[100] Svozil, Daniel, Vladimir Kvasnicka, and Jiri Pospichal. 1997. “Introduction to Multi-Layer Feed-Forward Neural Networks.” Chemometrics and Intelligent Laboratory Systems 39(1):43–62.

[101] Szegedy, Christian, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. 2015. “Going Deeper with Convolutions.” Pp. 1–9 in Proceedings of the IEEE conference on computer vision and pattern recognition.

[102] Tahaei, Hamid, Firdaus Afifi, Adeleh Asemi, Faiz Zaki, and Nor Badrul Anuar. 2020. “The Rise of Traffic Classification in IoT Networks: A Survey.” Journal of Network and Computer Applications 154:102538. doi: 10.1016/J.JNCA.2020.102538.

[103] Tang, Jie, Dawei Sun, Shaoshan Liu &. Jean-Luc Gaudiot. 2017. “Enable Deep Learning on IoT Deivces.” I E Ee Comput Er Soc I E T Y.

[104] Thakkar, Ankit, and Ritika Lohiya. 2021. “A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges.” Archives of Computational Methods in Engineering 28:3211–43.

[105] Thubert, Pascal, Carsten Bormann, Laurent Toutain, and Robert Cragie. 2017. IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header.

[106] Vincent, Pascal, Hugo Larochelle, Yoshua Bengio, and Pierre-Antoine Manzagol. 2008. “Extracting and Composing Robust Features with Denoising Autoencoders.” Pp. 1096–1103 in Proceedings of the 25th international conference on Machine learning.

[107] Winter, Tim, Pascal Thubert, Anders Brandt, Jonathan Hui, Richard Kelsey, Philip Levis, Kris Pister, Rene Struik, Jean-Philippe Vasseur, and Roger Alexander. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.

[108] Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. 2018. “IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?” IEEE Signal Processing Magazine 35(5):41–49.

[109] Kosrat Dlshad Ahmed & Shavan Askar, 2021. "Deep Learning Models for Cyber Security in IoT Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 61-70

[110] Yu, Adams Wei, Hongrae Lee, and Quoc V Le. 2017. “Learning to Skim Text.” ArXiv Preprint ArXiv:1704.06877.

[111] Yuen, Kevin Kam Fung. 2019. “Towards a Cybersecurity Investment Assessment Method Using Primitive Cognitive Network Process.” Pp. 68–71 in 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC).

[112] Zantalis, Fotios, Grigorios Koulouras, Sotiris Karabetsos, and Dionisis Kandris. 2019. “A Review of Machine Learning and IoT in Smart Transportation.” Future Internet 11(4):94.

[113] Zhang, Jun, Lei Pan, Qing-Long Han, Chao Chen, Sheng Wen, and Yang Xiang. 2021. “Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey.” IEEE/CAA Journal of Automatica Sinica 9(3):377–91.

[114] Tua Halomoan Harahap, Sofiene Mansouri, Omar Salim Abdullah, Herlina Uinarni, Shavan Askar, Thaer L. Jabbar, Ahmed Hussien Alawadi, Aalaa Yaseen Hassan, An artificial intelligence approach to predict infants’ health status at birth, International Journal of Medical Informatics, Volume 183, 2024, 105338, ISSN 1386-5056,

[115] Itika Sharma, Sachin Kumar Gupta, Ashutosh Mishra, Shavan Askar, “Synchronous Federated Learning based Multi Unmanned Aerial Vehicles for Secure Applications” Scalable Computing: Practice and Experience, Volume 2, No. 3, 2023.

[116] Media Ali Ibrahim; Shavan Askar, “An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm”, IEEE Access, Volume 11, 2023.

[117] Saman M. Omer, Kayhan Z. Ghafoor & Shavan K. Askar , “Lightweight improved yolov5 model for cucumber leaf disease and pest detection based on deep learning” Journal of Signal, Image and Video Processing, 2023

[118] Biju Theruvil Sayed, Mahmoud M. Al-Sakhnini, Asaad.A.H Alzubaidi, Ahmed H. R. Alawadi, Ahmed Jaber Ibrahim & Shavan Askar , “Assessment of Nano-Imprinting Process in CuZr Amorphous Films Through Combination of Machine Learning and Molecular Dynamics” Journal of Electronic Materials, Volume 52, 2023

[119] Shavan Askar, “Deep Forest Based Internet of Medical Things System for Diagnosis of Heart Disease”, ARO Journal, 2023.

[120] Omar Shirko; Shavan Askar , “A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking” IEEE Access, Volume 11, 2023.

[121] Shahab Wahhab Kareem , Bikhtiyar Friyad Abdulrahman , Roojwan Sc. Hawezi , Farah Sami Khoshaba , Shavan Askar , Karwan Muhammed Muheden , Ibrahim Shamal Abdulkhaleq, “Comparative evaluation for detection of brain tumor using machine learning algorithms” IAES International Journal of Artificial Intelligence (IJ-AI) Vol. 12, No. 1, March 2023.

[122] Dezheen H. Abdulazeez; Shavan K. Askar, “Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment” IEEE Accesss Volume 11, 2023.

[123] Saman M. Omer, Kayhan Z. Ghafoor, Shavan K. Askar, “Plant Disease Diagnosing Based on Deep Learning Techniques” ARO journal, 2022.

[124] SAMANN, Fady Esmat Fathel; Abdulazeez, Adnan Mohsin; Askar, Shavan. Fog Computing Based on Machine Learning: A Review. International Journal of Interactive Mobile Technologies (iJIM), [S.l.], v. 15, n. 12, p. pp. 21-46, jun. 2021.

[125] Kurdistan Ali & Shavan Askar, 2021. "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 101-115.