EAI Endorsed Transactions
on Smart Cities

Review Article EAI.EU

Design a framework for IoT- Identification, Authentication and Anomaly detection using Deep Learning: A Review

Aimen Shoukat[1], Muhammad Abul Hassan[2,*] , Muhammad Rizwan[3], Muhammad Imad[4], Farhatullah[5], Syed Haider Ali[6] and Sana Ullah[7]

[1]Department of Computer Science, Kinnaird College for WomenLahore Pakistan, aimen.shoukat007@gmail.com
[2]Department of Information Engineering and Computer Science, University of Trento, Italy. muhammadabul.hassan@unitn.it
[3]Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry CV4 7AL, UK, muhammad.rizwan.1@warwick.ac.uk
[4]Department of Computing and Technology, Abasyn University Peshawar, Imadk28@gmail.com
[5]School of Automation, China University of Geosciences, Wuhan 430074, China, farhatkhan8398@gmail.com
[6]Department of Electrical Engineering, University of Engineering and Technology Peshawar, engrsyedhaiderali@yahoo.com
[7]Department of Computer Science, Qurtuba University of Science and Technology, Peshawar Pakistan, sunnykhan3304@gmail.com

Abstract

The Internet of Things (IoT) connects billions of smart gadgets so that they may communicate with one another without the need for human intervention. With an expected 50 billion devices by the end of 2020, it is one of the fastest-growing industries in computer history. On the one hand, IoT technologies are critical in increasing a variety of real-world smart applications that can help people live better lives. The cross-cutting nature of IoT systems, on the other hand, has presented new security concerns due to the diverse components involved in their deployment. For IoT devices and their inherent weaknesses, security techniques such as encryption, authentication, permissions, network monitoring, \& application security are ineffective. To properly protect the IoT ecosystem, existing security solutions need to be strengthened. Machine learning and deep learning (ML/DL) have come a long way in recent years, and machine intelligence has gone from being a laboratory curiosity to being used in a variety of significant applications. The ability to intelligently monitor IoT devices is an important defense against new or negligible assaults. ML/DL are effective data exploration techniques for learning about 'normal' and 'bad' behavior in IoT devices and systems. Following a comprehensive literature analysis on Machine Learning methods as well as the importance of IoT security within the framework of different sorts of potential attacks, multiple DL algorithms have been evaluated in terms of detecting attacks as well as anomaly detection in this work. We propose a taxonomy of authorization and authentication systems in the Internet of Things based on the review, with a focus on DL-based schemes. The authentication security threats and problems for IoT are thoroughly examined using the taxonomy supplied. This article provides an overview of projects that involve the use of deep learning to efficiently and automatically provide IoT applications.

Keywords: IOT, DL, ML, Challenges, IoT Applications

Received on 19 July 2022, accepted on 17 November 2022, published on 17 January 2022

doi: 10.4108/eetsc.v7i1.2067

*Corresponding author. Email: muhammadabul.hassan@unitn.it

1. Introduction

Over the last decade, application devices such as smartphones, sensor systems, and controllers have become increasingly sophisticated, allowing for easier communication between devices as well as the completion of more complex tasks. In 2008, the number of system devices surpassed the global population [1], and the figure has continued to rise exponentially till now. Mobile phones, built-in systems, wireless connectivity, and practically every gadget in the Internet of Things (IoT) era are all linked to a local area network. The development of Internet-of-Things (IoT) devices, such as mobile phones [2], sensor technologies [3], sensor systems for uncommon aerial vehicles [4], [5], intellectually smart devices [6], and so on, has resulted in a slew of new apps on the cell phone as well as remote platforms. The amount of information gathered from these devices frequently grows in parallel with the range of devices. Innovative technologies are evolving that analyze data for practical interconnections and decision-making, eventually leading to Artificial Intelligence (AI) employing ML and Deep Learning DL algorithms.

In order to design effective IoT applications, we often use a workflow model that includes data collection, analysis, visualization, and evaluation [7], [8]. Data analysis is an important, computer-intensive component in which traditionally developed devices generally combine specialist knowledge and machine learning for classification and regression problems such as traffic forecasting, vehicle tracking, delivery time estimation, and so on. Moreover, as society moves into the "big data" era, existing approaches are unable to process large amounts of volatile and unpredictable data from hidden, incompatible IoT-based datasets. Almost all traditional methods focus on totally enclosed characteristics, and their effectiveness is strongly reliant on prior knowledge of specific locations. The majority of learning approaches employed in those devices use deep architectures with limited modeling and representational capacity. As a result, a far more powerful analytical tool is required to maximize the value of the priceless raw data generated by diverse IoT processes.

According to McKinsey's analysis of the worldwide economic ramifications of IoT, the yearly effect on the economy of IoT in 2025 will vary between $2:7 to $6:2 trillion. Healthcare accounts for 41% of the IoT sector, followed by the industry as well as oil, which accounts for 33% and 7% of the IoT sector, correspondingly. Transportation, agriculture, roads and bridges, security, and merchants account for about 15\% of the total IoT market. Such forecasts imply a massive and quick expansion of IoT services, data collection, and, consequently, demand in the future years. According to McKinsey's research, the economic impact of machine learning is defined as "the employment of computers to perform jobs that require complicated assessments, exact evaluations, and creative problem-solving." The research looks at the primary supporters of data automation in machine learning techniques like deep learning and neural networks.

The machine-to-machine connection can be short-range utilizing Wi-Fi, Bluetooth, or long-range using LoRa, M1 CAT, 4G, LTE, and 5G. Because IoT applications are used in so many different applications, the expense of IoT devices must be kept low. Moreover, IoT systems should be capable of performing basic functions such as data collecting, M2M connection, and so on. IoT is closely tied to "big data," as IoT systems continuously collect and exchange large amounts of data. For instance, an IoT platform employs technologies for managing, storing, and analyzing large amounts of data. It has become required in Infrastructure to deploy IoT services like Thingsboard, or Mainflux in order to support M2M communication via protocols including AMQP, and MQTT. As per the program, specific data processing must commonly occur on the Internet of things rather than on other centralized nodes inside the "cloud computing" system. The latest data processing model is known as "edge computing" is introduced as computation moves entirely to the end network nodes. Moreover, because these devices are frequently low-end, they might not have been suitable for intense applications. As a result, an intermediate node with sufficient capacities is needed to manage improved processing jobs that are spatially near the end network elements, reducing the load produced by huge data transmission to the number of inner cloud nodes. "Fog nodes" are presented in this work to aid large data handling on IoT devices by providing storage, computation, and networking services. Lastly, the data is kept within the cloud, where further testing using various ML and DL techniques, as well as sharing with other gadgets, results in the creation of smart apps with innovative value-added. Because traditional deep learning approaches do not match the current analysis requirements of IoT networks, DL has received a lot of attention. the structure of IoT data collection and processing necessitates the use of specialized traditional data analytics and AI approaches. Dl approaches were utilized to analyze big data in utilized the IoT cloud as well as streaming, as well as data from IoT devices and rapid data analytics in edge or fog computing.

Although IoT has already been done in recent years, deep learning in IoT applications is still in its early stages. Few researchers analyzed articles on wireless sensor networks (WSNs) with machine learning, integration of DL techniques for healthcare departments, DL methods and usability in IoT systems, and DL Techniques with their applications to build smart development. There is still no study that comprehensively investigates a broad range of IoT systems using DL after completing the survey on existing publications. We also believe that it is time to assess the current literature and use it to generate future study proposals. To that purpose, this paper outlines recent research including patterns in the use of deep learning techniques to enhance IoT systems. We'll show you how to use deep learning to improve IoT applications from a variety of angles. For instance, safety

monitoring, illness analysis, interior locations, artificial management, traffic prediction, home robots, vehicle automation, fault evaluation, and factory inspection. The concerns, constraints, and potential research areas for DL in IoT systems are also highlighted in order to stimulate as well as enable future discoveries in this promising field.

2. Background Theory

2.1 Concept of IoT systems

Today, an increasing number of products are connected to the internet in order to incorporate IoT perspectives in a variety of industries like smart buildings, public transportation, healthcare centers, industry, farming, and so on. In order to provide the buyers with IoT-system characteristics and specifications, the IoT framework gets converted entities in such domains from traditional to intellectual. To account for environmental modifications, specific frameworks must be altered during processes [9], [10]. IoT refers to all connected and constantly associated items, like electronic devices with sensors, and controllers, as well as a microprocessor integrated component. Because things need to communicate, which necessitates Machine-to-Machine interactions for short-range wireless systems like WiFi, Bluetooth, as well as ZigBee, the interaction range seems to be either restricted or broad when it comes to long-distance links like WiMAX, and GSM, as well as LTE [11]. The IoT is designed to give objects online identities that allow them to connect, share information, and access various resources. The concept of a digital identity for a large number of devices helps advanced Radio Frequency Identification systems advance (RFID). Such systems were built up as cheap computers due to their resource constraints, which prompted resource-constrained Wsns to emerge [12]. Highly networked equipment that may be altered as needed is an example of an IoT-enabled environment. The Internet of Things has been used to sustain patient recovery by following certain criteria, as well as to maintain patient characteristics. Furthermore, the findings can be used in researchers to compare patient exposure to various care settings on a worldwide basis [12].

The IoT can track and monitor energy consumption as well as provide entertainment. Food and agriculture production. It may measure and manage factors such as climate, political, atmospheric, farming, food, and animal disease elements. As the number of people with physical problems and life-threatening illnesses rises, so does the demand for IoT services and equipment [13].

2.2 Challenges of IoT

All transitions include benefits as well as challenges that must be overcome. These obstacles could be related to issues of protection, security, and so on. This section covers the various potential issues associated with IoT structural analysis. Another stumbling issue is the current network structure's incapacity to serve real-time essential IoT applications; as a result, SDN is seen as a suitable communication network for such applications [14],[15],[16],[17],[18],[19].

2.3 Deep Learning Algorithms in IoTs

Deep Learning is a sophisticated technique that is described as the latest update of ANN. It primarily focuses on building larger and more complicated neural networks with a large number of layers that are hidden that can handle massive amounts of data, like that found in photo pattern recognition, voice recognition, and IoT devices. The availability of cutting-edge IoT frameworks and accessible libraries for continuous monitoring, real-time processing, and secure storage of produced data such as photos, contingency tables, textual, voice, and video has resulted in a significant surge in IoT datasets [20] Various hardware systems functioning on the exterior or indoor ground-works, like smart urban sensors, smart organization fields, and so forth, generate such data. We require a distributed training model that is flexible and effectively utilizes the hardware resources of thousands of IoT devices to train such big-scale high-quality IoT data that's been gathered over a longer period in an acceptable amount of time.
The following are the most important deep learning algorithms:

1. Deep Neural Networks
2. Convolutions Neural Networks
3. Deep Boltzmann Machine

2.4 Applications of IoT

People can profit from the IoT in a variety of ways, including making life easier and assuring performance and safety. Healthcare equipment, city buildings, home automation systems, automobile design, electric utilities, as well as the smart world are all feasible applications. There are indeed countless applications in every part of existence since the introduction of super-duper and advanced technologies [21].

2.4.1 Health system

To improve the wellness of patients, new techniques have been created. Without touching the skin, diseases can be detected wirelessly and details displayed. Other sensors can measure pulse rate, blood oxygen, insulin levels, and temperature [22].

2.4.2 Smart Home

Traditional home appliances, such as fridges, washers, dryers, and Lightbulbs, have been designed with internet

access to help monitor and track equipment and to optimize energy usage with one another or with enrolled users. Aside from traditional technology, current inventions are gaining traction, such as smart house assistants, smart door locks, and so on [21].

2.4.3 Smart Transportation

It is possible to provide genuine help, save income, and cut emissions by using sensors built into automobiles or attached to city equipment to provide intelligent route advice, allocated parking, communications about traffic situations, telematics, as well as accident prevention [23].

2.4.4 Monitoring of Environmental Conditions

Any wireless sensor deployed across the city will be able to cope with a wide range of situations. Advanced weather stations can be made with other types of barometers and moisture sensors. Because smart sensors can detect pollution simultaneously at a range and at the molecular level, they are particularly valuable for monitoring the air quality and water emission levels in cities [24].

2.4.5 Management of Logistics and Supply Chains

The product's accessibility in manufacturing and retail is considerably reduced when RFID tags are used, lowering the total cost and time required. Active packaging characteristics such as product verification, customer quality management, client relationship, and customization are also necessary [25].

3 Identification

The initial necessity in IoT elements is identification, which serves as a confirmation of personal data for every object inside the IoT universe. The term "identity" is frequently used to refer to a specific person, equipment, or entity. Furthermore, it is regarded as an essential component in establishing a connection or interaction between persons, as well as for the success of an IoT system. It allows us to identify millions of disparate things and control them remotely over the Internet.
Identification also connects items to information about them that may be obtained from a server. It allows the item to interact with other objects with the same or opposite scopes via the Internet. To allow secure inter-object communication, there must be a method to align the identity of all Objects in the area. Based on the concepts that apply to item identity, identification management is necessary for three primary parties: the user, item identities, and connections. It must also address the IoT model's particular problems [26],[27],[28],[29],[30].

On the one side, identification is critical for IoT to define and correlate activities with their domain, as well as the issues of assigning a unique identity to each object and representing and preserving shared data. Identifying IoT objects, on the other hand, is required to distinguish between an item's ID or title and its address, which refers to the object's location within a communication network. For IoT devices, there are addressing techniques such as IPv4, IPv6, and 6LoWPAN addresses, and also numerous previous identifying methods such as RFID, Bluetooth, Barcode/2D code, and so on. Identification methods assign a distinct identification to each object in the network [27],[31],[32].

3.1 Deep Learning Use in IoT Identification

DL can enable IoT devices to read any information and effectively respond to both human and environmental situations, but performance in terms of energy consumption must be considered.
Some procedures have demonstrated the use of DP in IoT networks, like the work in [33], which used the deep learning methodology to select useful data from large amounts of multimedia information collected by IoT devices in a smart farming atmosphere, which is used to enhance farmers' standard of living. They still, however, see cloud computing as a way to deal with the energy and resource limits that come with implementing DL in IoT devices. They were also concerned about the network delays induced by such data [33].

Deep learning is also commonly employed in IoT applications including monitoring and object recognition. A large amount of data must be handled fast, and a speedy response is required. Cloud computing is unsuccessful in this scenario because it cannot satisfy the processing and reaction completion times. however, the issue can be fixed by utilizing fog computing, which can benefit both network edge as well as cloud resources. As a result of the work in [34], a DP-based fog cloud technology called EdgeLens has been developed for real object recognition in IoT application platforms.

Because deep learning has the potential to correctly handle any classification task, and identification is called a classification challenge, we assume that utilizing such approaches will produce in powerful and useful IoT item identity.

3.1.1 Methods of Earlier Identification

In the IoT context, all items must be identifiable in some way. To communicate with other things and share information in the same or distinct domains, each item should have a unique identity. In this section, we'll go over some of the previous ways of identifying IoT items.

1. Radio Frequency Identification (RFID)
2. Barcode/2D Code
3. Electronic Product Codes (EPC)

3.1.2 The Modern Identification Methods

This section presents an overview of the latest IoT object identification algorithms published over the last seven years.

1. Identification of Things Using Their Fingerprints
2. Computer Vision for Identification
3. Machine Learning Techniques for Identification

The ability to differentiate objects is the most significant feature of any IoT solution. Identification, which establishes evidence of identity information for every item in the Field of the IoT that normally identifies a unique item, including a person, equipment, or other entity, will be used to execute this. The object's distinct identity allows it to create, process, as well as exchange data with other entities of the same or opposite domain. As a result, the efficiency of IoT systems is determined by the identification method employed, making it critical to select a trustworthy identification scheme to achieve optimal system performance. However, the issue of establishing an appropriate identification technique for individual IoT platforms is a worry, as there is currently no universal identification mechanism that can be utilized for all IoT platforms.

The following research on existing object identification techniques in IoT indicates that many identifying methods, such as RFID, IP address, and others, have been employed since the IoT idea was introduced many years back. However, because the field's quick and continual expansion necessitates the development of identification methods as well, many new methods have lately been presented based on diverse methods such as computer vision, fingerprints, ML, and so on.

Although numerous approaches such as fuzzy systems, and artificial neural, including deep learning can be employed in a variety of sectors, they have yet to be applied to the identification of IoT devices, and if done successfully, will result in a huge change in the field.

4 Authorization

The user's accessibility to the IoT system is dependent on authorization. It allows only authorized clients to enter, monitor, and use data from IoT networks. The instructions of users with system authority are also carried out. It's difficult to maintain track of all user records and provide them access based on the data because clients are human, whereas sensors, equipment, and services are not.

Figure 1. Taxonomy of DP/ML-based AA for IoT.

Identification refers to a user's permission in an IoT infrastructure. Users must initially register to interact with the cloud server. But on the other hand, the trade-offs and reliability of IoT systems make identification difficult [35]. Phishing and masquerading attacks are also to blame for the network's vulnerability, and attackers will obtain access to the device rapidly if they don't provide enough identity. In a conclusion, to provide crucial protection when implementing system limitations, an adequate IoT system identification strategy is required [36].

Users & devices on the Internet are protected by two fundamental components: authentication and authorization. It makes such elements necessary for IoT deployment because the Internet of Things is nothing more than a collection of devices, ranging from simple sensors to vehicles and complex mobile devices, that connect to share information. Authenticity is a device identification method that verifies the authenticity of the device's customer Id and ensures that it is unique to that device. Authorization is a method of determining if a node (sensor node or user) is authorized to access things like reading or writing information, running programs, or operating devices. Connection denial or cancellation are also covered by authorization, especially if someone or something harmful is involved. In addition, permission allows you to link a particular device to specified services.

One sort of authentication & authorization process is for devices, while the other is for users. The focus of this research is on-device authentication and authorization. A

sensor is a great example of this. The device identity and permission level are defined through the AA processes before the communication session begins as well as the sensory information transfer takes place.

4.1 Anomaly Detection in IoT

There are situations where actual data sets are unique from all others and are identified as anomalies. Finding anomalies requires looking for things that are out of the ordinary in terms of activity when compared to normal nodes. Intrusion detection systems, fraud prevention, & data leaking are all separate sources of abnormalities. Anomaly detection is employed in a variety of IoT applications, like smart urban, network security, and industries [37], [38].

4.1.1 Intrusion detection

IoT devices are vulnerable to security attacks since they are connected to the Internet. DoS & DDOS attacks do severe damage to the IoT network. Identifying and preventing such threats is the most critical concern in IoT implementations [37], [39].

4.1.2 Fraud detection

When logins in or online payments, IoT systems are susceptible to receiving credit card information, banking info, or other sensitive information [37], [40].

4.1.3 Data leakage

External organizations can leak confidential information from a database, data centers, as well as other gathering procedures, directly threatening privacy as well as information loss. Such leaks can be avoided with proper encryption measures [37].

To address the gaps in the existing approaches, we propose designing an intrusion detection algorithm that is:

1. capable of detecting new forms of attacks
2. device-agnostic: it doesn't need to know what kind of device produced the network traffic. As a result, it can be used outside of the local network.
3. It is non-intrusive and privacy-preserving, in the sense that it does not spend time looking at application-level data. Then network traffic can be encoded without interfering with the examination.
4. delay-free: sometimes doesn't need to wait for an unknown period of time.

We build an IoT NIDS based on unlabeled data, especially anomaly identification techniques, in this section. As a result, our model is able to recognize new sorts of threats. We also look at two scenarios, based on whether or not it's important to figure out which device is causing the network traffic. We suggest employing a set of weak autoencoders to detect abnormal signals in IoT networks for such a reason. Autoencoder is an unsupervised neural network that can be used to detect anomalies, allowing new sorts of assaults to be detected. The data from communication networks is first preprocessed in order to extract important information. Normalization is also part of the pre-processing procedure. After that, the normalized information is passed into a series of weak autoencoders. We prepare a different weak autoencoder for every IoT device type present in the network since an IoT network is made up of highly various IoT device kinds. The autoencoder understands a device type's valid communication profile.

4.2 Machine Learning Techniques in IOT Detection

ML approaches like supervised [41], unsupervised [42], as well as reinforcement learning, can be used to detect unique threats in IoT devices and establish a good protection strategy. Multiple machine learning methods for IoT device protection. In machine learning, supervised learning is the most common strategy, in which the outcome is evaluated based on input using a qualifying set of data as well as a learning algorithm. Two different types of supervised learning are classification & regression modeling. There has been no outcome information for these input variables in unsupervised learning [41]. The majority of the data is unmarked, and the algorithm attempts to discover relationships between the various data sets. It divides them into clusters of different kinds Furthermore, Reinforcement learning allows the computer to learn from its own environment in the same way that some people do by doing actions that improve overall response. The feedback could be in the form of an award depending on the mission's outcome. In reinforcement learning, there are no predetermined behavior for any particular task, and the system relies on trial and error. By trial and error, the agent may discover and use the optimum plan from its knowledge to get the maximum reward [43].

5 Conclusion

A review of the DL and IoT methods used in many fields like home automation, smart city, smart transportation, power, localization, healthcare system, safety, agriculture, and others is discussed in this study. In recent years, analysts and business units have focused on DL and IoT, both of which have had a favorable impact on our lives, cities, and the environment. This review provides a thorough overview and sufficient knowledge of the many methods available for identification, as well as the benefits of employing them, which supports the decision to utilize a Deep Neural Network to design a novel and robust identification methodology for IoT items. The report establishes the groundwork for future research by employing ML/DL-based AA to collaboratively and unified address IoT security issues. To meet the crucial

criteria for IoT security, for example, the vast number of encryption methods needed for an AA process could be re-designed to be lighter, cooperative, and adaptable by utilizing ML/DL-based approaches. This study discusses a number of topics, including authentication protocol reliability, per-service authorization, set of data inaccessibility, overhead reduction through sharing of information, services-trust relationships, easy, period, and destination authentication schemes, as well as Reinforcement for AA.

References

[1] M. Swan, "Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0," Journal of Sensor and Actuator networks, vol. 1, no. 3, pp. 217-253, 2012.

[2] C. Cai, M. Hu, D. Cao, X. Ma, Q. Li, and J. Liu, "Self-deployable indoor localization with acoustic-enabled IoT devices exploiting participatory sensing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5297-5311, 2019.

[3] C. Wang, H. Lin, and H. Jiang, "CANS: Towards congestion-adaptive and small stretch emergency navigation with wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1077-1089, 2015.

[4] S. Lateef, M. Rizwan, and M. A. Hassan, "Security Threats in Flying Ad Hoc Network (FANET)," Computational Intelligence for Unmanned Aerial Vehicles Communication Networks, pp. 73-96, 2022.

[5] M. Hu et al., "On the joint design of routing and scheduling for vehicle-assisted multi-UAV inspection," Future Generation Computer Systems, vol. 94, pp. 214-223, 2019.

[6] M. Chen, F. Herrera, and K. Hwang, "Cognitive computing: architecture, technologies and intelligent applications," Ieee Access, vol. 6, pp. 19774-19783, 2018.

[7] A. Hussain, M. Imad, A. Khan, and B. Ullah, "Multi-class Classification for the Identification of COVID-19 in X-Ray Images Using Customized Efficient Neural Network," in AI and IoT for Sustainable Development in Emerging Countries: Springer, 2022, pp. 473-486.

[8] S. P. RM et al., "Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything," Journal of parallel and distributed computing, vol. 142, pp. 16-26, 2020.

[9] H. Zeyu, X. Geming, W. Zhaohang, and Y. Sen, "Survey on edge computing security," in 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2020: IEEE, pp. 96-105.

[10] F. E. F. Samann, S. R. Zeebaree, and S. Askar, "IoT provisioning QoS based on cloud and fog computing," Journal of Applied Science and Technology Trends, vol. 2, no. 01, pp. 29-40, 2021.

[11] S. Shehzadi, M. A. Hassan, M. Rizwan, N. Kryvinska, and K. Vincent, "Diagnosis of Chronic Ischemic Heart Disease Using Machine Learning Techniques," Computational Intelligence and Neuroscience, vol. 2022, 2022.K. Ali and S. Askar, "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, vol. 5, no. 3, pp. 101-115, 2021.

[12] O. Uviase and G. Kotonya, "IoT architectural framework: connection and integration framework for IoT systems," arXiv preprint arXiv:1803.04780, 2018.

[13] S. I. Ullah, A. W. Ullah, A. Salam, M. Imad, and F. Ullah, "Performance Analysis of POX and RYU Based on Dijkstra's Algorithm for Software Defined Networking," in European, Asian, Middle Eastern, North African Conference on Management & Information Systems, 2021: Springer, pp. 24-35.

[14] F. S. Fizi and S. Askar, "A novel load balancing algorithm for software defined network based datacenters," in 2016 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), 2016: IEEE, pp. 1-6.

[15] S. K. Askar, "Adaptive load balancing scheme for data center networks using software defined network," Science Journal of University of Zakho, vol. 4, no. 2, pp. 275-286, 2016.

[16] Ahmad, S. and Hassan, M., 2022. Secure Communication Routing in FANETs: A Survey. Studies in Computational Intelligence, pp.97-110.

[17] G. A. Qadir and S. Askar, "Software Defined Network Based VANET," International Journal of Science and Business, vol. 5, no. 3, pp. 83-91, 2021.

[18] S. Askar, G. Zervas, D. K. Hunter, and D. Simeonidou, "Adaptive classified cloning and aggregation technique for delay and loss sensitive applications in OBS networks," in 2011 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference, 2011: IEEE, pp. 1-3.

[19] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," Digital Communications and Networks, vol. 4, no. 3, pp. 161-175, 2018.

[20] H. U. Rehman, M. Asif, and M. Ahmad, "Future applications and research challenges of IOT," in 2017 international conference on information and communication technologies (ICICT), 2017: IEEE, pp. 68-74.

[21] A. Salam, F. Ullah, M. Imad, and M. A. Hassan, "Diagnosing of Dermoscopic Images using Machine Learning approaches for Melanoma Detection," in 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020: IEEE, pp. 1-5.

[22] I. Kök, M. U. Şimşek, and S. Özdemir, "A deep learning model for air quality prediction in smart cities," in 2017 IEEE International Conference on Big Data (Big Data), 2017: IEEE, pp. 1983-1990.

[23] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," Future Internet, vol. 11, no. 4, p. 94, 2019.

[24] M. A. Hassan, M. Imad, T. Hassan, F. Ullah, and S. Ahmad, "Impact of Routing Techniques and Mobility Models on Flying Ad Hoc Networks," in Computational Intelligence for Unmanned Aerial Vehicles Communication Networks: Springer, 2022, pp. 111-129.

[25] G. Alpár et al., "New directions in IoT privacy using attribute-based authentication," in Proceedings of the ACM International Conference on Computing Frontiers, 2016, pp. 461-466.

[26] E. Yadav and E. Ankur, "A survey of growth and opportunity of Internet of Things (IoT) in Global Scenario," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, pp. 20664-20671, 2016.

[27] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic Privacy-Preserving Identity Management System for the Internet of Things," Mobile Information Systems, 2017.
[28] M. Imad, F. Ullah, and M. A. Hassan, "Pakistani Currency Recognition to Assist Blind Person Based on Convolutional Neural Network," Journal of Computer Science and Technology Studies, vol. 2, no. 2, pp. 12-19, 2020.
[29] M. Rizwan et al., "Risk monitoring strategy for confidentiality of healthcare information," Computers and Electrical Engineering, vol. 100, p. 107833, 2022.
[30] M. A. Hassan, S. I. Ullah, A. Salam, A. W. Ullah, M. Imad, and F. Ullah, "Energy efficient hierarchical based fish eye state routing protocol for flying ad-hoc networks," Indonesian Journal of Electrical Engineering and Computer Science, vol. 21, no. 1, pp. 465-471, 2021.
[31] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless personal communications, vol. 58, no. 1, pp. 49-69, 2011.
[32] M. A. Hassan, A. R. Javed, T. Hassan, S. S. Band, R. Sitharthan, and M. Rizwan, "Reinforcing Communication on the Internet of Aerial Vehicles," IEEE Transactions on Green Communications and Networking, 2022.
[33] S. I. Ullah, A. Salam, W. Ullah, and M. Imad, "COVID-19 lung image classification based on logistic regression and support vector machine," in European, Asian, Middle Eastern, North African Conference on Management & Information Systems, 2021: Springer, pp. 13-23.
[34] H. R. Abdulqadir et al., "A study of moving from cloud computing to fog computing," Qubahan Academic Journal, vol. 1, no. 2, pp. 60-70, 2021.
[35] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2679-2689, 2019.
[36] B. Sharma, L. Sharma, and C. Lal, "Anomaly detection techniques using deep learning in IoT: a survey," in 2019 International conference on computational intelligence and knowledge economy (ICCIKE), 2019: IEEE, pp. 146-149.
[37] M. Imad, A. Hussain, M. A. Hassan, Z. Butt, and N. U. Sahar, "IoT Based Machine Learning and Deep Learning Platform for COVID-19 Prevention and Control: A Systematic Review," AI and IoT for Sustainable Development in Emerging Countries, pp. 523-536, 2022.
[38] Lateef, S., Rizwan, M. and Hassan, M., 2022. Security Threats in Flying Ad Hoc Network (FANET). Studies in Computational Intelligence, pp.73-96.
[39] H.-T. Pai, S.-H. Wang, T.-S. Chang, and J.-X. Wu, "Challenge of anomaly detection in IoT analytics," in 2020 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan), 2020: IEEE, pp. 1-2.
[40] M. Imad, S. I. Ullah, A. Salam, W. U. Khan, F. Ullah, and M. A. Hassan, "Automatic Detection of Bullet in Human Body Based on X-Ray Images Using Machine Learning Techniques," International Journal of Computer Science and Information Security (IJCSIS), vol. 18, no. 6, 2020.
[41] M.Imad, N. Khan, F. Ullah, M. A. Hassan, and A. Hussain, "COVID-19 classification based on Chest X-Ray images using machine learning techniques," Journal of Computer Science and Technology Studies, vol. 2, no. 2, pp. 01-11, 2020.
[42] Hassan, M., Ullah, S., Khan, I., Hussain Shah, S., Salam, A. and Ullah Khan, A., 2020. Unmanned Aerial Vehicles Routing Formation Using Fisheye State Routing for Flying Ad-hoc Networks. The 4th International Conference on Future Networks and Distributed Systems (ICFNDS).
[43] M. Imad, M. Abul Hassan, S. Hussain Bangash and Naimullah, "A Comparative Analysis of Intrusion Detection in IoT Network Using Machine Learning", Studies in Big Data, pp. 149-163, 2022. Available: 10.1007/978-3-031-05752-6_10.
[44] M. Hassan, S. Ali, M. Imad and S. Bibi, "New Advancements in Cybersecurity: A Comprehensive Survey", Studies in Big Data, pp. 3-17, 2022. Available: 10.1007/978-3-031-05752-6_1.