# Addressing IoT Security Challenges through AI Solutions

Md Shihab Uddin
School of Engineering
San Francisco Bay University
Fremont, CA 94539

## ABSTRACT

The Internet of Things (IoT) is a widely recognized technology that profoundly influences various sectors, including connectivity, work, healthcare, and the economy. IoT holds the potential to enhance daily life across different environments, from smart cities to educational settings, by automating processes, boosting efficiency, and reducing stress. However, the rise of cyberattacks and threats poses significant challenges to the security of intelligent IoT applications. Traditional methods for securing IoT are becoming increasingly ineffective due to emerging threats and vulnerabilities. To maintain robust security protocols, future IoT systems will require the integration of AI-powered machine learning and deep learning techniques. Leveraging the capabilities of artificial intelligence, particularly through machine learning and deep learning, is essential for equipping next-generation IoT systems with dynamic and adaptive security mechanisms. This paper explores IoT security intelligence from various perspectives, proposing an innovative approach that utilizes machine learning and deep learning to extract insights from raw data, thereby protecting IoT devices against a wide range of cyberattacks. It also discusses how these technologies can be employed to detect attack patterns in unstructured data and enhance the security of IoT devices.

## Keywords

Internet of things; cyberattacks; anomalies; deep learning; machine learning; security; data security; network security

## 1. INTRODUCTION

The Internet of Things (IoT) paradigm has gained popularity in recent years. At a conceptual level, IoT refers to the inter connectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness. IoT devices include personal computers, laptops, tablets, smart phones, PDAs, and other hand-held embedded devices. Devices now communicate smartly to each other or to us. Connected devices equipped with sensors and/or actuators perceive their surroundings, understand what is going on and perform accordingly [1] [2]. This is achieved by processing the sensed data at a node, device hub, or in a cloud. Devices are also enabled to take decisions autonomously or may propagate information to users, so that users can make the best decisions [2].

The interconnected device networks can lead to a large number of intelligent and autonomous applications and services that can bring significant personal, professional, and economic benefits [3. 4], resulting in the emergence of more data-centric businesses. IoT devices have to make their data accessible to interested parties, which can be web services, smart phone, cloud resource, etc.

## 2. LITERATURE REVIEW

The Internet of Things (IoT) is a key player in technological progress. The term "IoT" refers to the "Internet of Things," where "Things" are electronic devices connected to the internet. The Fourth Industrial Revolution, or Industry 4.0, is characterized by the increased automation of traditional industrial and manufacturing processes, with IoT being one of the advanced technologies driving this movement [11].

IoT refers to a network of objects that can connect to the internet and wireless networks to exchange data automatically. Various organizations and research groups define the IoT and smart environments from different perspectives. According to the authors, the IoT is composed of RFID-based digital information flows and physical components [12].

In the healthcare sector, the IoT is rapidly being adopted, offering the potential to enhance patient engagement, health outcomes, and access to care. However, the proliferation of IoT devices also introduces significant security, privacy, and safety risks for both patients and healthcare providers. Despite this, there is still limited research focused on mitigating the risks posed by IoT in healthcare. Recent studies have explored integrating secure application solutions with IoT devices in healthcare settings. Due to the sensitive nature of healthcare data, developing a specialized IoT application for healthcare is critical [13]. Current IoT opportunities in the healthcare industry are promising, particularly because of their sensing and measurement capabilities, including the low-energy variant of narrowband IoT (N.B. IoT). Due to its low energy consumption, N.B. IoT is favored in the healthcare sector. There are various concepts for utilizing N.B. IoT in healthcare, and it has gained popularity for its compatibility with cellular systems such as LTE. Consequently, N.B. IoT has become a viable option for healthcare-related applications in recent years. However, the primary challenges for N.B. IoT involve security measures and other system-related issues. If these challenges are adequately addressed, N.B. IoT could become one of the most feasible and widely adopted solutions for low-power, wide-area healthcare installations [14].

One of the many challenges faced by the Internet of Things, which connects a wide array of objects to networks to enable complex and intelligent applications, is ensuring user privacy and protecting against various attacks, such as spoofing, denial of service (DoS), jamming, and eavesdropping. The author explores the vulnerabilities within IoT systems and potential methods for securing IoT networks using machine learning techniques, including supervised learning, unsupervised learning, and reinforcement learning (RL). The analysis of data privacy emphasizes ML-based approaches for authenticating IoT devices, controlling access, securely offloading data, and detecting malware. The future adoption of IoT will have a substantial impact on society, business, and the economy. Since most nodes in an IoT network have limited resources, they are often targeted by hackers. Various solutions have been proposed to address IoT network security and privacy concerns, most of which rely on standard cryptographic protocols. However, these existing solutions are insufficient for addressing the unique security challenges posed by IoT networks. By incorporating machine learning (ML) and deep learning into IoT devices and networks, many threats to IoT security can be mitigated.

The current IoT opportunities in the healthcare sector are promising, especially due to its sensing and measuring capabilities, including the low-energy form of narrowband IoT. This technology is popular in the healthcare field because of its low energy usage. Several concepts exist for using narrowband IoT in the healthcare industry. Narrowband IoT has become widely used and is compatible with cellular networks like LTE. As a result, narrowband IoT has recently emerged as a viable choice for healthcare-related applications [15]. The IoT risk management model in healthcare is presented in Figure 1.

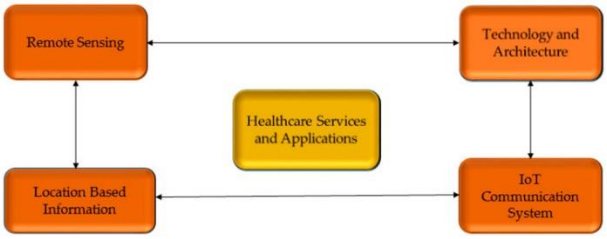
Remote Sensing
Technology and Architecture
Healthcare Services and Applications
Location Based Information
IoT Communication System

**Figure 1: The IoT risk management model in healthcare [16].**

.

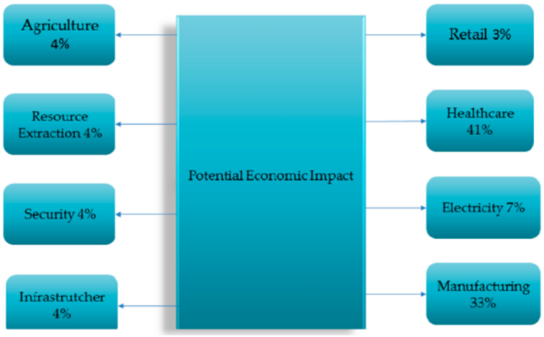

**Figure 2: Potential economic impact of dominant IoT applications by 2025 [22]**

## 3. SECURITY ISSUES IN THE SENSING LAYER

A typical IoT architecture is composed of three main layers: the application layer, the network layer, and the perception layer [23]. However, as the importance of data processing and intelligent decision-making continues to grow, the support or middleware layer between the network and application layers has become increasingly crucial. IoT systems can include multiple layers, such as a network layer and a support layer. In many studies on IoT systems, cloud computing has been utilized as the underlying support layer.

The perception layer, also known as the sensing layer, comprises various sensors and devices. This layer is characterized by limited storage, processing, memory, and communication capabilities. The primary security measures in this layer include node authentication, weak encryption, and access control [24]. Unfortunately, privacy attacks and crimes targeting the perception layer are prevalent in real-world scenarios. One common attack method involves taking control of a node. Other techniques include the use of malicious code, data injection, replay attacks, and side-channel attacks. For instance, if an attacker gains control of a node, it may cease to transmit valid network data and could even disable the IoT security software. If the IoT application receives corrupted data or is compromised by malicious code injection, it may not function as intended. Eavesdropping, also known as sniffing or snooping, is a technique where an attacker intercepts and examines data exchanged between two devices [25]. In an IoT network, a replay attack involves repeatedly falsifying, altering, or reusing the identities of related objects. Given sufficient time and access to encryption keys, an attacker can also perform a timing attack. These are just a few examples of the numerous ways vital information can be compromised beyond direct node attacks [26].

**Table 1: IoT Key Issues**

| Ref. | IoT key issues | Advantages |
|---|---|---|
| [34] | Quality of service (QoS) | Involves managing data traffic load and protocols across all layers in IoT architecture, including routine checks for QoS (Quality of Service) and QoE (Quality of Experience). |
| [35] | Authentication and identification | Focuses on addressing issues related to IoT integrations with internet protocols (IPv6), as well as authentication and identification issues. |
| [36] | Environment, power, and energy | Discusses the incorporation of green technology in IoT, the design of low-power-consumption devices and chips, and aspects of pollution control and management. |
| [37] | Reliability | Covers connectivity, mobility, and routing issues, along with the reliability of infrastructure and IoT applications. |
| [38] | Scalability | Discusses the challenges of scaling IoT solutions across large platforms and geographical locations, including potential discovery services. |

## 4. SECURITY ISSUES IN THE MIDDLEWARE OR SUPPORT LAYER

Distributed computing solutions have been used to replace centralized cloud environments in a variety of cases, with good results in terms of performance and response time. All sent data should now be checked for accuracy, concision, and secrecy. When someone inside a network purposefully alters or steals data or information, this is known as a malicious inside attack

[29]. By inserting malicious SQL queries into the code, SQL injection attacks are used to steal data from user services in the real world. When damage to one virtual machine spreads to another, this is a virtualization attack. With the help of cloud malware injection, a hacker can take over a cloud service, install malicious code, or even create a fake virtual machine. There could be significant consequences if attacks are so powerful that cloud infrastructure is incredibly frustrated [30].

# 5. APPLICATION LAYER

Defining and maintaining IoT applications, including their interactions with specific clients, fall under the scope of the application layer. One way to use IoT services is through a user interface. A computer, a smartphone, or any other Internet-enabled smart device could serve as an interface. The data that the middleware layer process is used by the application layer [31]. This holds for a wide range of application categories, including applications for smart homes, smart cities, industry, construction, and health. The security needs of an application may change depending on how it functions. When sending information on climate change forecasts as opposed to when conducting online banking, it is acceptable to expect a better level of security. The application layer must address various security challenges, such as attacks on access control, malicious code, programming, data leaks, service interruptions, application vulnerabilities, and software flaws [32]. Attacks that interrupt service, commonly referred to as “Distributed Denial of Service (DoS)” attacks, stop users from using IoT apps by sending a flood of requests to servers or networks. Threat actors could use sniffer software to monitor data being transmitted by IoT apps. Attacks that gain unauthorized access can seriously harm a system quickly by preventing users from using IoT-related services and wiping data [33-36].

# 6. IoT SECURITY SOLUTIONS BASED ON ML

ML is transforming IoT security by enabling real-time monitoring of network traffic to detect anomalies that may indicate security breaches. ML and DL models are also used for UAV detection [37, 38]. These models continuously analyze data patterns from connected devices, identifying deviations from typical behavior that could signal a cyber threat. This section reviews current trends in IoT security, presenting specific examples and case studies that illustrate how ML methodologies are applied in practical scenarios.

## 6.1 Anomaly Detection Systems

ML models are employed in IoT networks for anomaly detection, where they monitor network traffic in real-time to spot unusual patterns indicative of security breaches. These models are unique in their ability to learn and adapt, using historical data to recognize new and emerging threats [39, 40]. This adaptability ensures that security measures evolve in tandem with the changing nature of cyber attacks, enhancing the capability to preemptively identify potential threats and customize security protocols to the specific characteristics of each IoT network. This approach provides a more robust and responsive defense mechanism against a broad spectrum of cyber threats [41].

## 6.2 Predictive Maintenance in Industrial IoT

In modern industrial environments, the use of ML algorithms for the predictive maintenance of IoT devices has become increasingly important. This proactive maintenance strategy leverages the vast amounts of sensor data collected by IoT devices to predict and prevent equipment failures before they happen. IoT devices in industrial settings are equipped with various sensors that constantly monitor and gather data on the performance and condition of machinery, including parameters like temperature, vibration, and pressure. ML algorithms analyze this extensive data to detect patterns and anomalies that could indicate potential failures or malfunctions [42].

## 6.3 Smart Home Security Systems

In the rapidly advancing consumer market, ML has become a crucial technology for enhancing the security of smart home devices. The integration of ML into home security systems is revolutionizing the management of security in residential spaces. One of the primary applications of ML in this area is through advanced facial recognition technologies. Unlike traditional security systems that rely on static passcodes or keys, ML-powered systems can dynamically recognize the faces of residents and frequent visitors, offering a more personalized and secure experience. These systems continuously learn and improve their accuracy over time by analyzing the various faces they encounter. Additionally, smart security systems can learn and understand regular household patterns and routines, enabling them to detect anomalies or unusual activities, such as movement in an empty house or a door being opened at an odd hour. This feature is particularly useful for monitoring elderly family members or securing the home while away [43].

## 6.4 Automotive Security

Connected vehicles represent a major advancement in the automotive industry, integrating communication technologies into vehicles. These technologies enable cars to communicate with each other (V2V - vehicle-to-vehicle), with infrastructure (V2I - vehicle-to-infrastructure), and with other devices (V2X - vehicle-to-everything), improving overall transportation efficiency, safety, and convenience. Beyond security, ML algorithms can predict potential vehicle faults before they occur by analyzing historical data and identifying patterns that typically precede equipment failures. This predictive maintenance approach reduces the risk of malfunctions that could be exploited by cyber threats. However, while ML significantly enhances automotive security, it also presents challenges, such as ensuring the privacy of collected data, protecting against manipulation of ML models, and maintaining regular updates to keep pace with evolving cyber threats [44].

## 6.5 Healthcare

IoT devices, such as wearable health monitors, connected medical equipment, and patient tracking systems, are increasingly integral in the healthcare sector. These devices collect, transmit, and process vast amounts of sensitive patient data, making robust security measures essential. ML algorithms can enhance the security of data transmission between IoT devices and central servers by ensuring encryption standards and identifying potential intercepts or data leaks in real time. Additionally, ML can automate responses to security threats, such as temporarily restricting access or alerting security personnel upon detecting suspicious activity, thereby reducing the need for manual monitoring.

## 6.6 Supply Chain Monitoring

In supply chain management, ML models monitor the integrity of goods, particularly in sensitive industries, by detecting tampering or deviations in environmental conditions. This enhances supply chain security and reliability. ML models analyze data from various sources, including sensors and IoT devices attached to products or packaging, to ensure that goods remain in their intended state throughout the supply chain. This could involve monitoring for signs of tampering, damage, or unauthorized access to the products [45, 46].

## 7. IoT SECURITY SOLUTIONS BASED ON DL

Deep learning often employs multi-layer perceptrons (MLPs) and feed-forward artificial networks (FFANs). The traditional MLP architecture consists of three layers: the input layer, one or more hidden layers, and the output layer. In an AI network, each node in a layer is connected to a specific value in the preceding layer, ultimately linking back to the input layer. During model training, MLP utilizes backpropagation to adjust the internal weight values [47]. This MLP network is applied to analyze the NSL-KDD dataset for malware detection, explain IoT parameters, identify malicious traffic originating from IoT devices, and develop a model for intrusion detection [48].

Recurrent neural networks (RNNs) are another model type that uses neural feed-forward networks but includes an internal state or memory to manage sequential data effectively. This characteristic makes RNNs particularly useful for IoT security, natural language processing, and speech recognition [49]. IoT devices generate a significant amount of sequential data, such as time-varying information and network traffic flows. The recurrent connections in neural networks allow them to detect potential security vulnerabilities when a threat's communication patterns evolve over time. The RNN's ability to predict time series, supported by its long short-term memory (LSTM), enables it to recall previous inputs. For instance, LSTM-based recurrent networks can be used to identify and classify malicious applications and detect intrusions, along with other security-related tasks [50].

Various deep learning models and hybrid network models can be employed to detect and prevent malware, spoofing, and computer virus attacks across a wide range of IoT devices [51]. One such model is a deep belief network (DBN)-based security model, which can be used to safeguard IoT devices [52]. Researchers have explored multiple deep learning approaches, categorizing them as discriminative when human intervention is required and generative when none is needed. Hybrid systems may also be utilized when the data quality necessitates it [53-62].

## 8. CONCLUSION

This paper gives a review of the literature on IoT security awareness, focusing on the IoT model, IoT-based intelligent environments, and the security challenges addressed by machine learning solutions. We conducted an evaluation of the knowledge base surrounding IoT security intelligence, examining the IoT paradigm, smart environments built on IoT, associated security issues, and the machine learning solutions that can mitigate these problems. Securing IoT devices and systems requires a comprehensive analysis of IoT system architectures and the various cyberattacks that can compromise them layer by layer. In this study, we explored how different machine learning and deep learning technologies can be leveraged to enhance IoT security. For IoT security to be truly effective, it must be underpinned by machine learning or deep learning models that are driven by relevant data attributes.

## 9. REFERENCES

[1] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography", Proceedings of the 19th International Conference on Geoinformatics, pp. 1-5, 2011.

[2] Y. Yu, J. Wang and G. Zhou, "The exploration in the education of professionals in applied Internet of Things engineering", Proceedings of the 4th International Conference on Distance Learning and Education (ICDLE), pp. 74-77, 2010.

[3] J. Li, Z. Huang and X. Wang, "Countermeasure research about developing Internet of Things economy: A case of hangzhou city", Proceedings of the International Conference on E-Business and E-Government (ICEE), 2011

[4] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services, New York, NY, USA, 2015, pp. 21-28, doi: 10.1109/SERVICES.2015.12.

[5] Podder, P., Mondal, M., Bharati, S., & Paul, P. K. (2021). Review on the security threats of internet of things. arXiv preprint arXiv:2101.05614.

[6] Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and challenges of cloud integrated IoMT. Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, 67-85.

[7] Mondal, M. R. H., Bharati, S., Podder, P., & Kamruzzaman, J. (2023). Deep Learning and Federated Learning for Screening COVID-19: A Review. BioMedInformatics, 3(3), 691-713.

[8] Hoque, K., Hossain, M. B., Sami, A., Das, D., Kadir, A., & Rahman, M. A. (2024). Technological trends in 5G networks for IoT-enabled smart healthcare: A review. International Journal of Science and Research Archive, 12(2), 1399-1410.

[9] Bazgir, Ehsan, et al. "Security aspects in IoT based cloud computing." World Journal of Advanced Research and Reviews 20.3 (2023): 540-551.

[10] Mazhar, T., Talpur, D.B., Shloul, T.A., Ghadi, Y.Y., Haq, I., Ullah, I., Ouahada, K. and Hamam, H., 2023. Analysis of IoT security challenges and its solutions using artificial intelligence. Brain Sciences, 13(4), p.683.

[11] Rawat, D.B.; Doku, R.; Garuba, M. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security. IEEE Trans. Serv. Comput. 2019, 14, 2055–2072.

[12] Farrokhi, A.; Farahbakhsh, R.; Rezazadeh, J.; Minerva, R. Application of Internet of Things and artificial intelligence for smart fitness: A survey. Comput. Netw. 2021, 189, 107859.

[13] Yahya, F.; Zaki, A.F.A.; Moung, E.G.; Sallehudin, H.; Bakar, N.A.A.; Utomo, R.G. An IoT-based Coastal Recreational Suitability System using Effective Messaging Protocol. Int. J. Adv. Comput. Sci. Appl. 2021, 12, 8.

[14] Routray, S.K.; Gopal, D.; Javali, A.; Sahoo, A. Narrowband IoT (NBIoT) Assisted Smart Grids. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27March 2021; pp. 1454–1458.

[15] Sangra, P.; Rana, B.; Singh, Y. Energy efficiency in IoT-based smart healthcare. In Proceedings of Third International Conference on Computing, Communications, and Cyber-Security; Springer: Singapore, 2023; pp. 503–515.

[16] Alshamrani, M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. J. King Saud Univ. Comput. Inf. Sci. 2021, 34, 4687–4701.

[17] S. Bharati, M. R. H. Mondal and P. Podder, "A Review on Explainable Artificial Intelligence for Healthcare: Why, How, and When?," in IEEE Transactions on Artificial Intelligence, vol. 5, no. 4, pp. 1429-1442, April 2024, doi: 10.1109/TAI.2023.3266418.

[18] Bharati, S., Mondal, M. R. H., Podder, P., & Kose, U. (2023). Explainable artificial intelligence (XAI) with IoHT for smart healthcare: A review. Interpretable Cognitive Internet of Things for Healthcare, 1-24.

[19] Bharati, S., & Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and communication networks, 2022(1), 8951961.

[20] Khandoker Hoque, Md Boktiar Hossain, Denesh Das, Partha Protim Roy . Integration of IoT in Energy Sector. International Journal of Computer Applications. 186, 36 ( Aug 2024), 32-40. DOI=10.5120/ijca2024923981.

[21] Sarker, B., Sharif, N. B., Rahman, M. A., & Parvez, A. S. (2023). AI, IoMT and Blockchain in Healthcare. Journal of Trends in Computer Science and Smart Technology, 5(1), 30-50.

[22] Kaur, J.; Jaskaran; Sindhwani, N.; Anand, R.; Pandey, D. Implementation of IoT in Various Domains, in IoT Based Smart Applications; Springer: Berlin/Heidelberg, Germany, 2023; pp. 165–178.

[23] Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol. 2022, 100, 2988–3011.

[24] Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Bashir, A.K. A survey of security and privacy issues in the Internet of Things from the layered context. Trans. Emerg. Telecommun. Technol. 2020, 33, e3935.

[25] Navya, P.; Rama, G.S.; Kumar, T.P.; Pasha, S.N.; Mahender, K. IoT technology: Architecture, stack, security risks, privacy risks and its applications. In Proceedings of AIP Conference Proceedings; AIP Publishing LLC.: College Park, MD, USA, 2022; p. 020062.

[26] Chatterjee, U.; Ray, S. Security Issues on IoT Communication and Evolving Solutions. In Soft Computing in Interdisciplinary Sciences; Springer: Berlin/Heidelberg, Germany, 2022; pp. 183–204.

[27] Haque, A.K.M.B.; Bhushan, B.; Dhiman, G. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Syst. 2021, 39, e12753.

[28] Jangjou, M.; Sohrabi, M.K. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Arch. Comput. Methods Eng. 2022, 29, 3587–3608.

[29] Zahran, S.; Elkadi, H.; Helm,W. Fog of Things Framework to Handle Data Streaming Heterogeneity on Internet of Things. In Proceedings of International Conference on Advanced Intelligent Systems and Informatics; Springer International Publishing: Cham, Switzerland, 2022; pp. 653–667.

[30] Rasheed, M.A.; Saleem, J.; Murtaza, H.; Tanweer, H.A.; Rasheed, M.A.; Ahmed, M. A Survey on Fog computing in IoT. VFAST Trans. Softw. Eng. 2022, 9, 4.

[31] Yassein, M.B.; Shatnawi, M.Q. Application layer protocols for the Internet of Things: A survey. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–4.

[32] Donta, P.K.; Srirama, S.N.; Amgoth, T.; Annavarapu, C.S.R. Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. Digit. Commun. Netw. 2021, 8, 727–744.

[33] Kakkar, L.; Gupta, D.; Saxena, S.; Tanwar, S. IoT architectures and its security: A review. In Proceedings of the Second International Conference on Information Management and Machine Intelligence; Springer: Singapore, 2021; pp. 87–94.

[34] Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mob. Netw. Appl. 2018, 24, 796–809

[35] Nawalagatti, A. IoT: A Boon for Advancement of Technology. Int. J. Res. Appl. Sci. Eng. Technol. 2022, 10, 652–655

[36] Ja, S.; Dhasb, J.T.M.; Angelc, T.S. Proposed Novel Methodology for Automatic Drainage Block Identification in Smart Cities Using Internet of Things. In Advances in Parallel Computing Algorithms, Tools and Paradigms; IOS Press: Amsterdam, The Netherlands, 2022.

[37] Cˇ olakovic´, A.; Salihovic´, N.; Dželihodžic´, A. Adaptive Traffic Management Systems Based on the Internet of Things (IoT). In Proceedings of Advanced Technologies, Systems, and Applications VII: Proceedings of the International Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies (IAT) 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 426–437.

[38] Podder, P., Zawodniok, M., & Madria, S. (2024, June). Deep Learning for UAV Detection and Classification via Radio Frequency Signal Analysis. In 2024 25th IEEE International Conference on Mobile Data Management (MDM) (pp. 165-174). IEEE.

[39] Al-lQubaydhi, Nader, et al. "Deep learning for unmanned aerial vehicles detection: A review." Computer Science Review 51 (2024): 100614.

[40] Amit Deb Nath, Rahmanul Hoque, Md. Masum Billah, Numair Bin Sharif, Mahmudul Hoque . Distributed Parallel and Cloud Computing: A Review. International Journal of Computer Applications. 186, 16 ( Apr 2024), 25-32. DOI=10.5120/ijca2024923547

[41] Abusitta, A., de Carvalho, G.H., Wahab, O.A., Halabi, T., Fung, B.C. and Al Mamoori, S., 2023. Deep learning-enabled anomaly detection for IoT systems. Internet of Things, 21, p.100656.

[42] Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications.

[43] Huang, B., Chaki, D., Bouguettaya, A. and Lam, K.Y., 2023. A survey on conflict detection in iot-based smart homes. ACM Computing Surveys, 56(5), pp.1-40.

[44] Wang, X., Zhu, H., Ning, Z., Guo, L. and Zhang, Y., 2023. Blockchain intelligence for internet of vehicles: Challenges and solutions. IEEE Communications Surveys & Tutorials.

[45] E. Manavalan, K. Jayakrishna A review of internet of things (iot) embedded sustainable supply chain for industry 4.0 requirements Comput. Ind. Eng., 127 (2019), pp. 925-953

[46] Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P. and Fischl, M., 2021. Artificial intelligence in supply chain management: A systematic literature review. Journal of Business Research, 122, pp.502-517.

[47] Elghamrawy, S.M.; Lotfy, M.O.; Elawady, Y.H. An Intrusion Detection Model Based on Deep Learning and Multi-Layer Perceptron in the Internet of Things (IoT) Network. In International Conference on Advanced Machine Learning Technologies and Applications; Springer: Berlin/Heidelberg, Germany, 2022; pp. 34–46.

[48] Uhricek, D.; Hynek, K.; Cejka, T.; Kolar, D. BOTA: Explainable IoT Malware Detection in Large Networks; IEEE: New York, NY, USA, 2022; p. 1.

[49] Madhu, B.; Chari, M.V.G.; Vankdothu, R.; Silivery, A.K.; Aerranagula, V. Intrusion detection models for IOT networks via deep learning approaches. Meas. Sens. 2022, 100641.

[50] Al-Shareeda, M.A.; Manickam, S.; Saare, M.A. DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. Bull. Electr. Eng. Inform. **2023**, 12, 930–939.

[51] Gopal, S.B.; Poongodi, C.; Nanthiya, D.; Kirubakaran, T.; Logeshwar, D.; Saravanan, B.K. Autoencoder based Architecture for Mitigating Phishing URL attack in the Internet of Things (IoT) Using Deep Neural Networks. In 2022 6th International Conference on Devices, Circuits and Systems (ICDCS); IEEE: New York, NY, USA, 2022; pp. 427–431.

[52] Bhattacharya, S.; Ghorai, S.; Khan, A.K. Systematic Study of Detection Mechanism for Network Intrusion in Cloud, Fog, and Internet of Things Using Deep Learning. In Human-Centric Smart Computing; Springer: Berlin/Heidelberg, Germany, 2023; pp. 31–43.

[53] Saheed, Y.K.; Baba, U.A.; Orje-Ishegh, T.; Longe, O.B. An Efficient Machine Learning and Deep Belief Network Models for Wireless Intrusion Detection System. 2022.

[54] Hoque, K., Hossain, M. B., Sami, A., Das, D., Kadir, A., & Rahman, M. A. (2024). Technological trends in 5G networks for IoT-enabled smart healthcare: A review. International Journal of Science and Research Archive, 12(2), 1399-1410.

[55] Bharati, Subrato, et al. "Comparative performance analysis of different classification algorithm for the purpose of prediction of lung cancer." Intelligent Systems Design and Applications: 18th International Conference on Intelligent Systems Design and Applications (ISDA 2018) held in Vellore, India, December 6-8, 2018, Volume 2. Springer International Publishing, 2020.

[56] Javed Mehedi Shamrat, F. M., Tasnim, Z., Chowdhury, T. R., Shema, R., Uddin, M. S., & Sultana, Z. (2022). Multiple cascading algorithms to evaluate performance of face detection. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021 (pp. 89-102). Springer Singapore.

[57] Javed Mehedi Shamrat, F. M., Ghosh, P., Tasnim, Z., Khan, A. A., Uddin, M. S., & Chowdhury, T. R. (2022). Human Face recognition using eigenface, SURF method. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021 (pp. 73-88). Springer Singapore.

[58] Kowsher, M., Tahabilder, A., Sanjid, M. Z. I., Prottasha, N. J., Uddin, M. S., Hossain, M. A., & Jilani, M. A. K. (2021). LSTM-ANN & BiLSTM-ANN: Hybrid deep learning models for enhanced classification accuracy. Procedia Computer Science, 193, 131-140.

[59] Hoque, R., Maniruzzaman, M., Michael, D. L., & Hoque, M. (2024). Empowering blockchain with SmartNIC: Enhancing performance, security, and scalability. World Journal of Advanced Research and Reviews, 22(1), 151-162.

[60] Hoque, R., Billah, M., Debnath, A., Hossain, S. S., & Sharif, N. B. (2024). Heart Disease Prediction using SVM. International Journal of Science and Research Archive, 11(2), 412-420.

[61] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things, 11, 100227.

[62] Chowdhury, I. K., & Yu, W. B. (2024). Information extraction from the reviews of AI applications using SAS text Mining Process. Issues in Information Systems, 25(4), 127-135.