www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-11, Issue-6, December 2023
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Unlocking Network Security and QoS: The Fusion of SDN, IoT, and Machine Learning: A Comprehensive Analysis

S. Aleem[1]*, S. Ahmed[2]

[1]Dept. of Computer Science, Khwaja Moinuddin Chishti, Language university, Lucknow, India
[2]Dept. of Computer Science, Integral University, Lucknow, India

Corresponding Author: saimaaleem@kmclu.ac.in, Tel: 8887732045

Received: 05/Sept/2023, Accepted: 09/Nov/2023, Published: 31/Dec/2023

***Abstract*—**The convergence of Software-Defined Networking (SDN) and the Internet of Things (IoT) has ushered in transformative changes, offering unparalleled levels of network flexibility, programmability, and connectivity. While this integration provides numerous benefits, it also introduces security challenges. Motivated by the imperative to fortify the security posture in this dynamically evolving landscape, this review paper explores the vulnerabilities, threats, and corresponding responses in the security landscape of SDN and IoT. Recognizing the critical need for proactive security measures, the paper underscores the potential of Quality of Service (QoS) empowered by Machine Learning (ML) as a solution. By harnessing ML, QoS emerges as a powerful means to proactively identify and mitigate potential attacks, offering an effective approach to enhance network security. The motivation behind integrating QoS with ML lies in its ability to ensure dependability, availability, and integrity, thereby instilling confidence in the reliability and resilience of the interconnected world.

The paper goes through examination of challenges, delving into the proactive management of QoS within SDN, intricacies of IoT network architectures, and the unique features and limitations of IoT systems. Furthermore, it comprehensively addresses potential countermeasures for various security threats, such as Denial of Service (DOS), Man-in-the-Middle (MITM) attacks, and Ransomware attacks, particularly on devices with limited resources. This abstract provides a concise yet comprehensive overview of the paper's motivations, emphasizing the urgency and significance of the proposed solutions for securing modern network environments.

***Keywords*—**SDN, IoT, QoS, ML, DOS, MITM, WSN, M2M.

I. INTRODUCTION

The convergence of Software-Defined Networking (SDN) and the Internet of Things (IoT) has brought about a transformative shift in our technological interaction, offering unparalleled levels of network flexibility, programmability, and connectivity. This dynamic integration has ushered in numerous advantages, enabling centralized network control and administration while facilitating real-time data exchange between the digital and physical realms. However, as is often the case with technological progress, it has also introduced new challenges, particularly in the realm of security [1]. The Quality of Service (QoS) paradigm, bolstered by the capabilities of Machine Learning (ML), emerges as a promising avenue for tackling the emerging security threats associated with SDN and IoT [2]. Through proactive identification and mitigation of potential attacks, QoS with ML offers an effective approach to bolster network security, ensuring the dependability, availability, and integrity of services within this interconnected landscape. This study delves into the vulnerabilities, threats, and corresponding responses pertinent to the security landscape of SDN and IoT. Moreover, we highlight the game-changing potential of Machine Learning in bolstering security in both SDN and IoT environments. The fusion of ML with QoS offers a powerful safeguard, instilling confidence in the reliability and resilience of the interconnected world.

II. BACKGROUND

Ensuring optimal network performance is achieved through Quality of Service (QoS), a crucial element that facilitates the prioritization of traffic by providing dedicated bandwidth, reducing jitter, and minimizing latency [4]. In the face of escalating connected devices and data traffic, the significance of service quality within software-defined networking (SDN) has risen to a critical level [5][6]. The distinct separation of control and data planes in SDN offers a landscape of flexibility, programmability, and streamlined network administration [7].

The convergence of the Internet of Things (IoT) and machine learning (ML) with SDN brings about an elevated level of service quality enhancement. IoT contributes by enabling real-time data collection and analysis, thereby gaining insights into network activities and user preferences. Complementing this, ML algorithms foresee and optimize network performance, proactively identifying

potential issues and delivering tailored user experiences. To counteract risks, security protocols like firewalls, antivirus software, encryption, and multi-factor authentication are employed [8].

The convergence of Software-Defined Networking (SDN) and the Internet of Things (IoT) has ushered in groundbreaking services such as real-time traffic management and predictive maintenance [9]. The integration of advanced analytics fueled by machine learning with IoT data has led to improved quality of service within both IoT and SDN networks. Leveraging insights from machine learning, IoT devices and applications are empowered to make intelligent decisions. In SDN networks, machine learning plays a pivotal role in enhancing quality of service by identifying anomalies, facilitating real-time threat detection, and categorizing network traffic. Through traffic analysis and optimization, it fortifies both quality of service and overall network functionality, thereby ensuring secure QoS within SDN networks [10].

[10] and [11] offer valuable insights into prevailing IoT routing protocols, security strategies, and the ongoing research challenges. Additionally, [12] introduces a software-based security architecture centered on "mboxes" and a centralized security controller for efficient IoT security management. Addressing network security challenges, these encompass malware attacks, phishing attempts, Denial of Service (DoS) attacks, man-in-the-middle attacks, and password-related breaches [13]. The author[14] systematically identified and characterized a spectrum of Man-In-The-Middle (MITM) attacks, each exhibiting distinct behaviors, as evidenced by the existing literature. These attacks encompass a range of tactics including message tampering, message delaying, and message dropping. The analysis undertaken by the author provides a comprehensive understanding of the multifaceted nature of MITM attacks, shedding light on the diverse ways in which adversaries can exploit vulnerabilities to manipulate, disrupt, or intercept communications.

III. LITERATURE REVIEW

The Internet of Things (IoT) has pervaded numerous facets of daily life, prompting the development of energy-efficient data aggregation techniques for IoT-WSN systems. As the scope of IoT broadens, the need arises for service models that can classify applications and identify requisite Quality of Service (QoS) elements. Wireless sensor networks (WSNs) play a pivotal role in ensuring service quality within the IoT landscape, necessitating the exploration of integration strategies while upholding QoS standards. A security-aware framework was introduced by Author [15] to counter saturation attacks within the SDN stack and safeguard network services against Denial-of-Service (DoS) attacks. They validated its efficacy through experiments involving various DoS/Flooding attack tools and real-world attack scenarios, assessing impacts on TCP, UDP/IP, HTTP, and NTP services. Nonetheless, effectively managing the multitude of sensor nodes in WSNs poses challenges, underscoring the demand for efficient, scalable approaches capable of accommodating dynamic network alterations and node behaviors [16].

In a comprehensive article [17], the origins and broader implications of the SDN architecture are elucidated, particularly its interconnection with Network Function Virtualization (NFV). The piece also delves into areas for prospective research, encompassing security, 5G, AI integration, IoT, and energy efficiency. By spotlighting tangible use cases and identifying key challenges, the paper aspires to stimulate further exploration and progress within the realm of Software Defined Networking. Capitalizing on the SDN controller's programmability, network operators and clients are endowed with extensive programming interfaces capable of encapsulating intricate infrastructure aspects [18]. This attribute holds the potential to simplify network forwarding actions and regulations by employing more adaptable high-level policy languages, diverging from exclusive protocols or manufacturer-specific command sets. When sharing data among a substantial number of participants, various considerations, including effectiveness, data accuracy maintenance, and the preservation of data owner privacy, come to the fore [19]. Concerns arise among certain users regarding data sharing and privacy protection, especially in systems lacking anonymity, which can expose users to vulnerabilities like tracking and spoofing attacks . As the pervasive utilization of IoT systems introduces a fresh array of security challenges, conventional security techniques such as encryption, authentication, and access control prove inadequate for addressing the vulnerabilities of IoT devices. Consequently, there is an imperative to enhance existing security methods to fortify the IoT ecosystem. Recent strides in machine learning and deep learning have transformed these technologies from experimental concepts to practical tools with applications across diverse critical domains [20]. With the escalating number of Internet of Things (IoT) devices, machine learning (ML) has gained traction for monitoring and alerting users about security threats [22]. Central to IoT network security is the concern of malicious intrusions. Several machine learning strategies have been developed to detect such intrusions. Early efforts introduced a robust SVM-based solution for intrusion detection , leveraging the DARPA Basic Security Module dataset from 1998. A more recent approach proposed a hybrid detection method amalgamating SVMs, uniting misuse and anomaly detection models [24]. For identifying malicious behaviors, particularly those grounded in time-series patterns, a pragmatic approach employing RNN, particularly LSTM, has been put forward [25]. The frequent interconnection of IoT devices with Android mobile devices has contributed to a surge in malware authors striving to compromise devices for remote control.

Various machine learning techniques, including CNN, autoencoder-based approaches, and SVM-based malware detection, have been tailored to counter the threats posed by

malware. These techniques assume a pivotal role in ensuring dependable IoT services [26][27]. Yet, a considerable challenge arises from the inconsistent portrayal of IoT architecture, which engenders difficulties in comprehending security nuances [28]. In the realm of IoT security, machine learning methods hold promise, but several significant challenges remain unaddressed. The absence of uniformity in articulating IoT architecture constitutes a notable impediment when grappling with security apprehensions [29]. In contrast, IoT systems must balance their core functions with the diverse demands of various applications [30]. Achieving this equilibrium entails IoT designs harnessing fitting protocols and access networks, while embracing adaptable service-oriented architectures that cater to diverse quality factors [31].

In their study [32], the author delves into the factors influencing Quality of Service (QoS) within Delay-Tolerant Networks (DTNs). Insights from the literature reveal that congestion, selfish behaviors, fair resource allocation, queuing delay, and jitter collectively impact QoS, influencing metrics such as delivery ratio, packet drop rate, message overhead, and delay within DTNs. The integration of service-oriented architectures enhances IoT's flexibility, adeptly catering to varied service requirements while upholding core functionality. The immense data generation by IoT is efficiently processed by the cloud, and as an ecologically mindful alternative, fog computing comes to the fore, offloading tasks to nearby edge devices [30]. The fusion of software-defined networks (SDN) and fog computing directly addresses fog-related challenges, thereby augmenting QoS. Additionally, wireless sensor networks (WSNs) offer promising real-time applications due to their compact size, cost-effectiveness, and simplified installation procedures [33].

In the realm of Delay Tolerant Networks (DTNs), intermittent connectivity poses challenges to ensuring Quality of Service (QoS) [35]. QoS metrics, encompassing delivery ratio, packet drop, message overhead, and delay, are influenced by factors like congestion, selfishness, fairness, queuing delay, and jitter within DTNs. Despite the existence of various QoS systems, none comprehensively address all dimensions. Particularly for real-time Internet applications, the assurance of latency, bandwidth, and loss rate guarantees holds paramount importance. However, the intricate interplay of packets complicates QoS in packet-switched networks. Notably, QoS frameworks such as Integrated Service (IntServ) and Software-Defined Networking (SDN) have been explored, with the dynamic queue mapping in SDN showing promise.

Furthermore, the challenge of enabling communication across diverse networking environments, exemplified by the Interplanetary Internet merging terrestrial and interplanetary links, remains intricate [36]. A protocol-based architecture grounded in the "least common denominator" approach simplifies application development, setting it apart from conventional Internet protocols. The core principles of this delay-tolerant networking (DTN) architecture, centered on the Bundling protocol, offer a pathway to streamlined scalability [36], promising more manageable expansion compared to other alternatives.

Simultaneously, a novel approach [37] introduces inventive methods for delivering fractional bandwidth channels within service classes not conventionally associated with such channels. By adeptly classifying frames and prioritizing QoS circuits, this strategy optimizes delivery, particularly in systems like Fibre Channel Class 2 and Class 3. Noteworthy components such as CPU, ports, queues, and processors play pivotal roles in this process, alongside the potential for a holistic network fabric.

Meanwhile, another study [38] delves into diverse outcomes stemming from quality-of-service factors within various RPL networks. This exploration consistently elevates network performance and quality, as evidenced by indicators predicting strength, dependability, stability, and flexibility. The analysis, conducted through simulations with the Contiki Cooja Simulator, highlights how RPL-based IoT networks can enhance their quality of service with an increasing number of nodes.

Furthermore, in [39], an investigation revolves around the RPL Routing Protocol for Low-Power and Lossy Networks (LLNs) within the context of the Internet of Things (IoT). This study contrasts the operating modes—storing and non-storing—of LLN network elements constrained by processor capacity, memory, and battery limitations. The scrutiny of RPL behavior in relation to various quality-of-service standards in wireless sensor networks (WSNs) utilizes simulations. Notably, the results accentuate the trade-offs between energy consumption and performance, highlighting the nuanced interplay between the modes' advantages and drawbacks.

In a pioneering effort, [40] presents a technique merging SDN and machine learning for identifying flow resources in applications, achieving an impressive 97.6% accuracy in dynamic bandwidth allocation without requiring controller processing or content analysis. Addressing the potential of the Internet of Things (IoT), [41] surveys its enabling technology, unsettled issues, and socio-environmental considerations, categorizing research contributions and outlining forthcoming challenges. The exploration of wireless sensor networks (WSNs) in [43] emphasizes dynamic self-configuration, behavior analysis, and challenges such as scalability, cost, and communication dynamics. Investigating IoT security and standards, [44] focuses on the five-layer protocol stack, while [45] underscores the role of queueing theory in designing wireless sensor networks for IoT. Additionally, [46] offers a comprehensive analysis of IoT methodologies, architectures, and data challenges, while [47] maps quality-of-service approaches, pinpointing trends and areas for improvement in IoT research.

.In reference [48], the authors comprehensively tackled the data security risks posed to the Internet of Things (IoT)

landscape. Their exploration extended to potential defense mechanisms, thoughtfully incorporating advanced technologies tailored to the heterogeneous and resource-limited IoT ecosystems. However, the discussion fell short in addressing the pressing concern of resource constraints, neglecting strategies pertaining to the outsourcing or delegation of computational tasks. Their methodology involved categorizing threats spanning perception, network, and application layers, adeptly presenting corresponding preventive measures. While delving into lightweight end-to-end communication security methods, their coverage appeared somewhat constrained when it came to crucial topics such as access control, data integrity approaches, and their seamless integration within IoT systems.

Simultaneously, The author [49] introduces an innovative approach based on Host Identity Protocol (HIP) to establish comprehensive end-to-end security between sensor nodes and Internet hosts within the Internet of Things (IoT) context. This solution adeptly takes into account the unique constraints of Wireless Sensor Networks (WSNs). The proposed framework entails adapting the communication and computational demands of the HIP protocol to suit the limited capabilities of sensor nodes, thus achieving a resilient and streamlined security mechanism.

Similarly, reference [50] witnessed another author's categorization of threats across the perception, network, and application layers within the IoT domain. Their assessment uncovered limitations in prevailing authentication, authorization, identification, trust, and privacy methods tailored for IoT devices. Yet, a comprehensive resolution to address these shortcomings remained absent. Collectively, these articles not only highlight the intricate challenges and potential solutions surrounding IoT security but also underscore the need for continued research to bridge existing gaps in various dimensions.

IV. SECURITY THREATS AND POTENTIAL COUNTERMEASURES.

Table 1. Attacks/Threads and possible counter measures.

Threat/Attack	Description and Possible Countermeasures
Denial of Service (DOS)	This type of attack aims to disrupt users' access to a system or its data by targeting the availability of the system or data. Employing diverse strategies can help mitigate the impact of such attacks. For instance, an effective approach involves clustering essential servers or services, which can include duplicating or triplicating them.[13]
Man-in-the-Middle Attack (MITM)	During a Man-In-The-Middle (M-I-T-M) attack, a malicious entity eavesdrops on a conversation and could manipulate the discussion, deceiving both parties into thinking they are communicating directly. Common countermeasures against this type of attack involve cryptographic solutions, including mutual authentication processes and encryption methods.[14]
Ransomware Attack	This form of malware is designed to encrypt or otherwise restrict access to data on a targeted computer. One of the commonly recommended strategies to safeguard against such attacks involves regularly backing up data and establishing disaster recovery plans to ensure business continuity.[16]
Security Attack on Devices with Limited Resources	It limits computing power of IoT sensors and devices poses a hurdle for employing traditional encryption algorithms effectively. To tackle this challenge, solutions include adopting lightweight cryptographic techniques and potentially offloading a segment of the encrypting and decrypting tasks to more capable computational devices.[29]
Hardware: Semi-Invasive and Invasive Attacks	Malicious attacks targeting device hardware have taken various forms, including extracting the package and utilizing infrared emission from the backside to pinpoint the vulnerable point of attack. Subsequent actions involve using a laser to manipulate bits and bypass encryption. Similarly, techniques like micro-probing and modifying chips through a focused ion beam (FIB) have been employed to breach hardware security . To counteract such threats, ensuring robust physical security measures for devices becomes essential. Implementations could range from safeguarding against tampering to restricting hardware access through secure placements and effective locking mechanisms [28].

V. INTERNET OF THINGS

The Internet of Things (IoT) is a network of real-world items, including furniture, machinery, cars, and buildings, equipped with electronics, sensors, and network connections to gather and share data. These connected devices create a system that can be monitored and managed remotely, making them smarter, more efficient, and autonomous. IoT enables smart homes, connected cars, wearable technologies, and industrial automation, improving decision-making and productivity. From common household items to high-tech business gear, IoT encompasses a wide range of physical objects embedded with software and sensors for **communication** and data exchange through the internet.[52]

Fig 1. Characteristics of IoT

A. IoT Network Architecture:

Network architecture encompasses both the logical and structural blueprint of a network, incorporating elements such as software, wireless networks, protocols, hardware, and connections. In the context of the Internet of Things (IoT), this architectural framework extends to the arrangement and coordination of devices, sensors, and components. It encompasses the orchestration of physical hardware, data connections, network routing, data transmission, and device interfaces. Key security measures like encryption and authentication are seamlessly integrated. Among the several IoT architectures, notable ones include the centralized, decentralized, edge computing, and hybrid architectures.

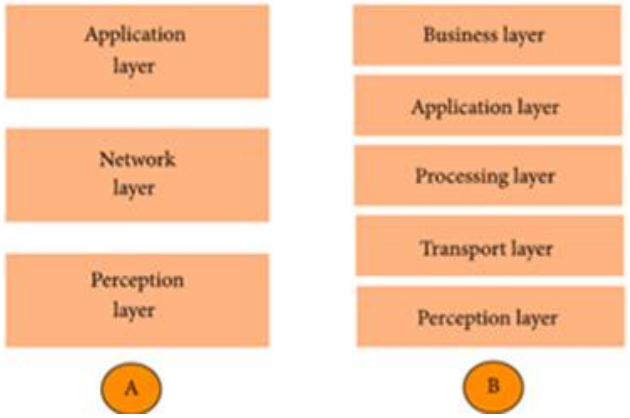

Fig 2. IoT Architecture (A: 3 Layer , B: 5 Layer).

The architecture of an IoT network holds paramount significance in determining its usability, reliability, and security. It should be intricately tailored to cater to the unique demands of the specific application or use case at hand. Flexibility is a cornerstone of IoT design, allowing devices to dynamically interact and communicate in real-time, even as they migrate. Furthermore, the essence of IoT lies in its diversity and decentralized nature. Sensor arrays measuring pressure, temperature, humidity, and other variables play a pivotal role. Data garnered from these IoT sensors is channeled to cloud servers through IoT gateways. This network is characterized by cost-effective yet intelligent devices, empowering them to autonomously communicate and interact. The ability for IoT nodes to be accessible from other nodes is an essential feature.

While the proliferation of IoT brings about a multitude of advantages, it also introduces certain inherent risks. Across various IoT architectures, distinctive layers are taken into account: the Cloud Layer, which encompasses remote server networks for on-demand storage, management, and processing of IoT data; the Middleware Layer, hosting mechanisms that facilitate seamless resource integration and interoperability; the Application Layer, responsible for governing network data flow and error handling; the Network Layer, which adeptly manages congestion and packet sequencing via switching and routing activities; the Link Layer, tasked with encoding and decoding data packets, as well as overseeing physical layer issues, flow, and frame synchronization; and finally, the Physical Layer, which enables the transmission and reception of data through cables and physical characteristics by physical sensors.

B. IoT Features and Limitations: A Comparative Analysis

The Internet of Things (IoT) encapsulates a dynamic landscape of services and versatile cross-platform technology, fostering dynamic interactions between interconnected devices. This framework efficiently gathers and analyzes data across IoT services, while cross-platform technology facilitates application development across diverse platforms [20]. This synergistic combination forms the bedrock of a robust IoT ecosystem, delivering heightened operational efficiency, stringent safety protocols, and seamless interconnectivity. Key attributes of IoT devices include scalability, robust safety measures, adaptability to dynamic changes, and the capacity to navigate the diverse network and device landscape. Notably, connectivity and interconnectivity play pivotal roles, ensuring uninterrupted data access and harmonious integration within IoT systems.

However, alongside its transformative potential, the IoT landscape presents distinct limitations that must be considered. The IoT's capacity to connect myriad smart devices across diverse domains is unparalleled, yet this very ubiquity can transform advantages into challenges. Interoperability issues emerge from the plethora of device manufacturers, leading to compatibility concerns. Moreover, secure and dependable networks are not uniformly available, potentially hindering the seamless connectivity that IoT devices necessitate. The energy dependence of numerous IoT devices on batteries raises concerns about power consumption and rapid depletion. Effective data management becomes a challenge, given the voluminous data generated by these devices. Scalability complications arise as the IoT ecosystem expands continuously. Security emerges as a critical concern, with many devices lacking even basic protections, weak authentication mechanisms, and limited encryption.[42] Furthermore, the physical accessibility of IoT devices renders them susceptible to tampering, while the potential collection of sensitive data raises serious privacy risks if mishandled. Therefore, while IoT's promise is immense, a comprehensive understanding of its features and limitations is imperative to harness its potential while addressing its inherent challenges.

VI. EXPLORING QOS IN SDN, IOT, AND ML

Quality of Service (QoS) entails orchestrating traffic-handling mechanisms within a network to align with service requisites for specific applications and users, guided by network policies. Resource allocation among clients and applications takes precedence in QoS management, addressing parameters such as bandwidth, delay, packet loss, and jitter. Bandwidth delineates connection speed, amenable to allocation for various traffic queues. Delay, the time packets take to reach their destination, can be

minimized through priority queues. QoS-driven decisions determine which packets to discard, countering packet loss due to network congestion. Jitter, arising from varying packet arrival times under congestion, is managed to ensure seamless audio and video transmissions. The importance of QoS varies across applications, with levels ranging from best-effort service to soft and hard QoS[23]. Strategies like overprovisioning and buffering aid in achieving high QoS. Software-Defined Networking (SDN) revolutionizes QoS management by centralizing network control through its architecture's data, control, and application planes, yielding dynamic control and heightened visibility. Incorporating SDN with IoT designs enhances network administration efficiency, separating control and data planes for optimized routing across IoT layers. This automation bolsters network performance and flexibility. Thorough planning ensures IoT device and protocol compatibility, as QoS remains pivotal for critical applications demanding efficient event management and inter-level communication. The integration of Software-Defined Networking (SDN) and the Internet of Things (IoT) has ushered transformative shifts in networking and cybersecurity [21]. However, these advancements necessitate addressing crucial security concerns. SDN's centralized control and programmability facilitate dynamic risk detection and mitigation, enhancing network management flexibility. Conversely, IoT's vast device network introduces vulnerabilities from non-standard protocols, insecure practices, and remote locations. Machine Learning (ML) assumes a pivotal role in cybersecurity, detecting anomalies and potential threats. The synergy of SDN, IoT, and ML enhances QoS by forecasting traffic patterns and optimizing resource allocation [51]. One notable framework employs supervised and unsupervised ML techniques to secure QoS in SDN-based IoT networks by identifying network irregularities. SDN and IoT networks face risks from DOS and DDOS attacks, impacting performance and service. ML-based methods counteract these threats by learning from network traffic patterns, autonomously deploying defenses against anomalies.

VII. CONCLUSION

In conclusion, the convergence of Software-Defined Networking (SDN) and the Internet of Things (IoT) presents a paradigm shift in technological interaction, offering unprecedented levels of network flexibility, programmability, and connectivity. While this integration offers numerous advantages, it also introduces new challenges, particularly in terms of security. The Quality of Service (QoS) paradigm, bolstered by Machine Learning (ML), emerges as a promising avenue for mitigating the emerging security threats associated with SDN and IoT. By proactively identifying and addressing potential attacks, QoS with ML offers an effective approach to enhance network security, ensuring the dependability, availability, and integrity of services within this interconnected landscape. This study has explored the vulnerabilities, threats, and corresponding responses relevant to the security landscape of SDN and IoT. Moreover, it has highlighted the transformative potential of Machine Learning in fortifying security in both SDN and IoT environments. The fusion of ML with QoS serves as a potent safeguard, instilling confidence in the reliability and resilience of the interconnected world. As the IoT ecosystem continues to evolve, ongoing research and innovation remain essential to address the multifaceted challenges and opportunities that arise. Through the continuous development of security protocols, interoperability standards, and the application of advanced technologies like Machine Learning, the vision of a secure and seamlessly connected IoT landscape can be realized.

REFERENCES

[1] Restuccia, F., D'Oro, S., Melodia, T. "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet Things J, vol. **5**, no**. 6,** pp. **4829–4842**, Dec. 2018, doi: 10.1109/JIOT.2018.2846040.

[2] Nauman, A., Qadri, Y. A., Amjad, M., bin Zikria, Y., Afzal, M. K., Kim, S. W. "Special Section On Mobile Multimedia: Methodology And Application Multimedia Internet Of Things: A Comprehensive Survey," pp**. 1-54**, doi: 10.1109/ACCESS.2020.2964280.

[3] Miorandi, D., Sicari, S., de Pellegrini, F., Chlamtac, I. "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol**. 10**, no. 7, Elsevier B.V., pp. **1497–1516**, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[4] Sarker, I. H., Hoque, M. M., Uddin, M. K., Alsanoosy, T. "Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions," Mobile Networks and Applications, vol. 26, no. 1, 2021, doi: **pp 285–303** , 10.1007/s11036-020-01650-z.

[5] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N., Qin, J. "A survey on the application of machine learning for the Internet of Things," International Journal of Machine Learning and Cybernetics, **vol. 9,** no. 8, 2018, pp **1399-1417,** doi: 10.1007/s13042-018-0834-5.

[6] Hammad, K., Moubayed, A., Primak, S. L., Shami, A. "QoS-Aware Energy and Jitter-Efficient Downlink Predictive Scheduler for Heterogeneous Traffic LTE Networks," IEEE Trans Mob Comput, vol. **17,** no. 6, 2018, pp **1468 - 1483** doi: 10.1109/TMC.2017.2771353.

[7] Bhat, O., Gokhale, P., Bhat, S. "Introduction to IOT," International Advanced Research Journal in Science, Engineering and Technology ISO, vol. **3297,** no. 1, 2007, pp **41-44** , doi: 10.17148/IARJSET.2018.517.

[8] Mudgal, S., Pranjale, S., Mahajan, V. "Impact of Cyber-Attacks on Economy of Smart Grid and their Prevention," U.Porto Journal of Engineering (2022), pp. **51 – 64,** DOI: 10.24840/2183-6493_008.002_0005.

[9] Qin, Q., Poularakis, K., Tassiulas, L. "Bringing Intelligence at the Network Data Plane for Internet of Things Security," "IoT for Defense and National Security," 2022, Publisher Willey , pp- ch **14** doi: 10.1002/9781119892199.

[10] Nguyen, K. T., Laurent, M., Oualha, N. "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. **32,** pp**. 17–31,** Sep. 2015, doi: 10.1016/j.adhoc.2015.01.006.

[11] Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). "Secure routing for Internet of Things: A survey." Journal of Network and Computer Applications, pp **198-213** doi: 10.1016/j.jnca.2016.03.006.

[12] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2016). "On the Security and Privacy of Internet of Things Architectures and Systems." In Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015, pp. **49–57**. doi: 10.1109/SIOT.2015.9.

[13] Zhang, C., & Green, R. (2015). "Communication security in Internet of Things: Preventive measure and avoid DDoS attack over IoT network." Simulation Series, 47(3), pp **8–15.**

[14] Lygerou, I., Srinivasa, S., Vasilomanolakis, E., Stergiopoulos, G., & Gritzalis, D. (2023). "Correction to: A decentralized honeypot for IoT Protocols based on Android devices." International Journal of Information Security, 21(6), pp **1211-1222**. doi: 10.1007/s10207-022-00605-7.

[15] Krishnan, P., & Achuthan, K. (2019). "Managing network functions in stateful application aware SDN." Communications in Computer and Information Science. Pp **88-103**, doi: 10.1007/978-981-13-5826-5_7.

[16] Hossen, M. A., & Sang, J. Y. (2019). "Q-Learning Based Multi-Objective Clustering Algorithm for Cognitive Radio Ad Hoc Networks." IEEE Access., pp **181959** - 181971 doi: 10.1109/ACCESS.2019.2959313.

[17] Schaller, S., & Hood, D. (2017). "Software-defined networking architecture standardization." Computers Standards & Interfaces, 54, pp **197–202**. doi: 10.1016/j.csi.2017.01.005.

[18] Lara, A., Kolasani, A., & Ramamurthy, B. (2014). "Network innovation using OpenFlow: a survey." IEEE Communications Surveys and Tutorials, 16(1),pp **493–512.** doi: 10.1109/SURV.2013.081313.00105.

[19] Huang, X., et al. (2015). "Cost-effective authentic and anonymous data sharing with forward security." IEEE Transactions on Computers, 64(4), pp **971–983**. doi: 10.1109/TC.2014.2315619.

[20] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security." IEEE Communications Surveys and Tutorials, 22(3), pp **1646–1685.** doi: 10.1109/COMST.2020.2988293.

[21] F Restuccia, S D'Oro, & T Melodia," Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking" IEEE Internet of Things Journal, 5(6), PP **4829-4842.** doi: 10.1109/JIOT.2018.2831526.

[22] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Syst Appl, vol. 41, no. 4 PART 2, pp. **1690–1700,** 2014, doi: 10.1016/j.eswa.2013.08.066.

[23] D Rahmati; S A Hamid, "Classified Round Robin: A Simple Prioritized Arbitration to Equip Best Effort NoCs With Effective Hard QoS," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, issue 1, pp. **257 - 269,** January 2018. DOI: 10.1109/TCAD.2017.2693263.

[24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," Computer Networks, vol. 76, pp. **146–164**, Jan. 15, 2015. doi: 10.1016/j.comnet.2014.11.008.

[25] N. McLaughlin et al., "Deep android malware detection," in CODASPY 2017 - Proceedings of the 7th ACM Conference on Data and Application Security and Privacy, Mar. 2017, pp. **301–308.** doi: 10.1145/3029806.3029823.

[26] S. Skorobogatov, "Compromising device security via NVM controller vulnerability," 2020 IEEE Physical Assurance and Inspection of Electronics (PAINE), Washington, DC, USA, 2020, pp. **1-6,** doi: 10.1109/PAINE49178.2020.933

[27] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE 2011, 2011. Pp art. no. **5940923** doi: 10.1109/WIRELESSVITAE.2011.5940923.

[28] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering." Pp 1-**10.**

[29] Renya Nath N, Hiran V Nath. "Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges," IEEE Computers and Electrical Engineering, Volume 100, pp **2-17,** May 2022.

[30] I. Ahammad, M. A. Rahman Khan, Z. U. Salehin, M. Uddin, and S. J. Soheli, "Improvement of QoS in an IoT ecosystem by integrating fog computing and SDN," International Journal of Cloud Applications and Computing, vol. 11, no. 2, pp. **48–66,** Apr. 2021, doi: 10.4018/IJCAC.2021040104.

[31] G. Kurt et al., "A Vision and Framework for the High-Altitude Platform Station (HAPS) Networks of the Future," Jul. 2020, pp **729-799.**

[32] A. Roy, T. Acharya, and S. DasBit, "Quality of service in delay tolerant networks: A survey," Computer Networks, vol. 130. Elsevier B.V., pp. **121–133,** Jan. 15, 2018. doi: 10.1016/j.comnet.2017.11.010.

[33] F. S Biswas, "QOS-AWARE SCHEDULING," United State Patent, Patent no. US 9,135,072 B2, Sep. 2015, Corpus ID: 44736585, pp **1-10 .**

[34] J. A. C. Gary G. Warden, "Systems and methods for providing quality of service (QoS) in an environment that does not normally support QoS features," Jun. 2008. Pp **1-12.**

[35] S. Kalyani, "Measurement and Analysis of QoS Parameters in RPL Network," 2018, pp. **307-312.**

[36] M. Sedrati, "Evaluation of QoS parameters with RPL protocol in the internet of things," in ACM International Conference Proceeding Series, **Jul. 2017**, vol. Part **F130657**, pp. 86–91. **doi: 10.1145/3129186.3129204.**

[37] M. R. Parsaei, M. J. Sobouti, S. Raouf, and R. Javidan, "Network Traffic Classification using Machine Learning Techniques over Software Defined Networks," 2017. Pp 219-225.

[38] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, vol. **144.** Elsevier B.V., pp. **17–39,** Oct. 24, 2018. doi: 10.1016/j.comnet.2018.07.017.

[39] Y. Yamsanwar and S. Sutar, "Performance analysis of wireless sensor networks for QoS," in 2017 International Conference on Big Data, IoT and Data Science, BID 2017, 2018, vol. **2018-January,** pp **120-123,** doi: 10.1109/BID.2017.8336584.

[40] Vivek S., "Performance analysis of FMAC protocol for reporting rate in wireless sensor networks," 2016, pp**1-5 .**

[41] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Communications Surveys and Tutorials, vol. **17**, no. 3, pp. **1294–1312**, Jul. 2015, doi: 10.1109/COMST.2015.2388550.

[42] M Díaz, C Martín, & B Rubio" State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing." Journal of Network and Computer Applications, vol. **67,** pp **99-117.**

[43] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of things: A review of surveys based on context aware intelligent services," Sensors (Switzerland), vol. 16, no. 7. MDPI AG, Jul. 11, 2016.pp **1-23,** doi: 10.3390/s16071069.

[44] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," Journal of Systems and Software, vol. 132, pp. 1**86–203,** Oct. 2017, doi: 10.1016/j.jss.2017.05.125.

[45] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. **118–137**, Apr. 2018, doi: 10.1016/j.dcan.2017.04.003.

[46] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Computer Networks, vol. 148, 2019, pp **283- 294** doi: 10.1016/j.comnet.2018.11.025.

[47] T. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," IEEE Communications Surveys and Tutorials, vol. 10, no. 4. 2008, pp **56-76,** doi: 10.1109/SURV.2008.080406.

[48] S A Fadhil,". Internet of Things security threats and key technologies. Journal of Discrete Mathematical Sciences and Cryptography, Pages **1951-1957**, 25 Oct 2021.

[49] Sahraoui, S., & Bilami, A. (2015). Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. Computer Networks, Volume **19** 14 November 2015, PP **26-45.**

[50] S. Chen and K. Nahrstedt, "An Overview of Quality-of-Service Routing for Next-Generation High-speed Networks: Problems and Solutions." Pp **64-79.**

[51] M. U. Akram, M. Rizwan Asghar, M. A. Naeem, H. A. Khan, and H. Farooq, "Secure QoS Provisioning for SDN-based IoT Networks using Machine Learning," IEEE Access, vol**. 9**, pp. **11120-11136**, 2021. DOI: 10.1109/ACCESS.2021.305113.

[52] K. K. Patel, & S. M Patel," Internet of Things (IoT): Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges" International Journal of Engineering Science and Computing, **May 2016**, PP- **6122-6131.**

[53] P Sethi, S R Sarangi, " Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering" Volume **2017,** Article ID 9324035. Pp **1-25** , doi: 10.1155/2017/9324035.

AUTHORS PROFILE

Mrs. Saima Aleem is an Assistant Professor at Khwaja Moinuddin Chishti Language University in Lucknow since July 2020. Currently, she is actively engaged as a co-project investigator in a research initiative supported by the Department of Higher Education, Uttar Pradesh Government. In her academic journey, she is pursuing a Ph.D. scholar at Integral University. Saima Aleem's areas of research expertise span across domains, encompassing Computer Networks, Artificial Intelligence, e-Services, and e-Governance.

Dr. Shish Ahmed is an Associate Professor in the Department of Computer Science and Engineering at Integral University in Lucknow, India, Shish Ahmad's research is focused on light-weight network security, sensor networks, MANET, cloud computing, IoT, and big data. He has a Ph.D. in Computer Science and Engineering from Integral University, an MTech in Computer Science from U.P. Technical University, and a B.E. in Computer Engineering and Information Technology from M.J.P. Rohial Khand University. Shish Ahmad has over 20 years of teaching and research experience, and his work has resulted in three awarded and five working Ph.D. supervisions and two patents. He has published 3 papers in SCI/SCI-E journals, 9 papers in SCOPUS-indexed journals, and 15 papers in Google Scholar/peer-reviewed international journals. Additionally, he has presented papers at five international conferences and book chapters, and his papers have been cited 135 times in Google Scholar, 28 times in Scopus, and 18 times in the Web of Science. Shish Ahmad has also attended several short-term courses, workshops, and seminars on topics such as effective teaching, academic leadership, cloud infrastructure, networking, and more.

