International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 170-176, November-2023

https://doi.org/10.47001/IRJIET/2023.711024

StreamSafe: Improving QoS and Security in IoT Networks

[1]Sathiamoorthy A., [2]Mithusan S., [3]Rathnayaka R.M.L.R., [4]Kajenthiran S., [5]Mahaadikara M.D.J.T. Hansika [6]Dinithi Pandithage

[1,2,3,4]Dept. of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka
[5,6]Dept. of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

***Abstract* - This research project takes a holistic strategy to improve QoS and security in SDN-based IoT networks. We offer an intricate solution with a federated autoencoder-based tool to precisely identify malicious network traffic in response to the expanding IoT ecosystem and its security issues. We use a QoS dashboard coupled with OpenDaylight to monitor latency, throughput, packet loss, and jitter, dynamic resource allocation based on device priorities, and better MQTT AES encryption. These elements constitute a framework for SDN-based IoT networks' changing needs. Global autoencoder models with client models on IoT devices provide real-time anomaly detection in our system. We offer a packet manipulator to generate tailored network traffic samples for robust model training. The OpenDaylight-integrated QoS dashboard gives administrators real-time network performance data. A priority-based resource allocation system allocates resources by device significance to preserve QoS during peak demand. AES encryption for MQTT, a popular IoT standard, is also improved. It protects critical IoT data from security risks. Our Mininet-based Ubuntu simulations show that our technique maintains QoS, detects network anomalies, and strengthens IoT network security. These findings show that our methodology may improve SDN-based IoT deployment reliability and security, creating a more resilient and secure ecosystem.**

Keywords: Internet of Things (IoT), Quality of Service (QoS), Software-Defined Networking (SDN), Anomaly Detection, OpenDaylight, Dynamic Resource Allocation, AES, MQTT.

I. INTRODUCTION

The Internet of Things (IoT) represents a transformative era where interconnected devices exchange data to enhance their cognitive capabilities, transforming ordinary objects into intelligent entities. This proliferation of IoT has brought about numerous benefits, improving industrial efficiency, resource utilization, healthcare outcomes, and daily living standards [1]. However, this expansion also raises significant security concerns that traditional approaches cannot adequately address [2]. Machine learning (ML) has emerged as a valuable tool in IoT security, enabling the analysis of extensive datasets to identify patterns and behaviors indicative of potential security vulnerabilities [3]. This study recognizes the critical importance of security and Quality of Service (QoS) in Software-Defined Networking (SDN) and IoT networks. IoT connections between devices and sensors, connecting residential, communal, and industrial sectors, create complex, heterogeneous networks with significant data volumes, presenting challenges to information security. The study's primary goal is to comprehensively investigate security and QoS in SDN-IoT networks. It focuses on deploying a federated architecture rooted in deep learning for an artificial intelligence intrusion detection system. Additionally, advanced AES encryption within the MQTT protocol enhances security, while a priority-based bandwidth allocation system and real-time QoS monitoring further optimize IoT networks' performance. This research aims to bridge the gap between the potential of IoT technology and the critical need for robust security and efficient network performance in this increasingly interconnected world.

II. RELATED WORK

Internet of Things (IoT) networks are inherently heterogeneous, with diverse devices using various communication protocols and hardware constraints. This diversity leads to challenges in decentralized, peer-to-peer connections, potentially causing issues like reduced throughput, speed, and increased packet loss [4]. Security in IoT networks becomes critical to prevent malicious devices from accessing sensitive data, necessitating protective measures. Software-Defined Networking (SDN) offers a solution to enhance Quality of Service (QoS) management and resource governance in IoT networks [5]. SDN controllers dynamically allocate bandwidth to meet IoT device QoS requirements [6]. LoRa technology, a common wireless access platform for IoT networks, has unique radio connection properties and protocol stack limitations, posing QoS challenges [7]. Research has explored QoS indicators in LoRa networks, focusing on Packet Delivery Ratio (PDR), End-to-End Delay, and Energy Consumption. The impact of

LoRaWAN variables like data rate, retransmissions, and transmission power on these parameters is also studied. Furthermore, QoS-aware routing algorithms integrate mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) into the IoT framework, considering aspects like delay, reliability, energy efficiency, and load balancing [8]. SDN's potential in IoT networks is evident, enhancing scalability, QoS, and security, with research covering various aspects, including architectures, protocols, and algorithms [5]. Federated learning (FL) is a privacy-preserving method that addresses data privacy concerns and collaboration limitations in distributed on-device training [9]. FL allows devices to gain knowledge without sharing raw data, enhancing IoT device security and minimizing communication delays by selectively transmitting data to the server [10], [11].Table 1 provides an overview of FL-based solutions and their constraints.

TABLE 1: COMPARISON OF FL-BASED SOLUTIONS

Authors	Use case	Limitations
Cetin et al. [12]	Intrusion detection solution based on FL for IoT networks	Basic model and performance is not analyzed
Nguyen et al. [13]	Self-learning anomaly detection for IoT networks	Data privacy is not considered
Attota et al. [14]	IoT scalable intrusion detection with FL	No comparison with other ML and DL techniques
Friha et al. [15]	FL in agricultural intrusion detection system (IDS)	FL-based IDS was not test for decentralized models
Zhao et al. [16]	Multi-task network anomaly detection using FL	No information on detailed experimentation
Lian et al. [17]	Decentralized FL-based IDS	No comparison to neural networks.

Quality of Service (QoS) in Software-Defined Networking (SDN) and Internet of Things (IoT) networks relies on traffic shaping, bandwidth allocation, and flow control mechanisms. Traffic shaping restricts IoT traffic flow, while bandwidth allocation evenly shares network resources. Effective flow control mitigates congestion and manages IoT data influx. SDN-IoT networks use bandwidth allocation and management techniques to optimize resource use. Previous research explored hierarchical allocation algorithms tailored for SDN-IoT networks, factoring in architecture and traffic load to improve resource distribution [18]. Studies focused on bandwidth allocation in SDN-IoT networks, emphasizing dynamic and priority-based methods. These initiatives employ dynamic allocation systems with feedback loops to optimize bandwidth allocation based on real-time demand. Priority-based bandwidth allocation is gaining popularity to meet IoT device QoS requirements [19]. Hybrid systems combining dynamic and priority-based approaches are becoming more widespread. This study analyzes hybrid methodologies that adjust bandwidth allocation based on varying traffic situations and prioritize IoT device QoS standards, establishing a robust QoS framework for SDN-enabled IoT networks. While IoT offers significant potential, it requires robust security measures to protect data and prevent breaches [20]. Traditional encryption methods are often inadequate due to device limitations, unreliable networks, and the need for rapid communication in IoT settings. AES encryption integrated with MQTT has gained prominence for securing IoT communications [21]. The Advanced Encryption Standard (AES) is known for its robust security and efficient performance. AES encryption within MQTT protects IoT data from unauthorized access and interception [22]. This study aims to analyze enhanced security measures' principles, methods, and benefits [23]. The ultimate goal is to establish secure and reliable communication in the evolving IoT landscape.

III. METHODOLOGY

This section delineates the methodology employed in our research. This study proposes a federated deep learning-based intrusion detection system, real-time quality of service (QoS) metrics monitoring, priority-based bandwidth optimization, and advanced AES encryption integration with MQTT protocol. Our research framework focuses on each component's methods and concerns.

3.1 Federated deep learning-based intrusion detection system

Released in March 2018, the N-BaIoT dataset fills a void in publicly available datasets for IoT botnet attacks [24]. This multivariate, sequential dataset contains data from nine commercial IoT devices compromised by the Mirai and BASHLITE botnets. It includes 7,062,606 instances of network traffic data, each with 115 real-valued metrics. This dataset supports the development of intrusion detection algorithms tailored for IoT environments. Deep learning models are crucial for detecting network anomalies due to IoT devices' unique attributes and constraints [25]. Deep autoencoders are well-suited for this purpose as they capture intricate patterns in high-dimensional data and reduce dimensionality [26]. These models excel at anomaly detection, adapt to different IoT environments, and work efficiently on resource-constrained devices. Leveraging the PyTorch framework, known for its deep learning capabilities and adaptability, simplifies implementing federated. Figure 1.1 shows the proposed federated architecture.

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 170-176, November-2023
https://doi.org/10.47001/IRJIET/2023.711024

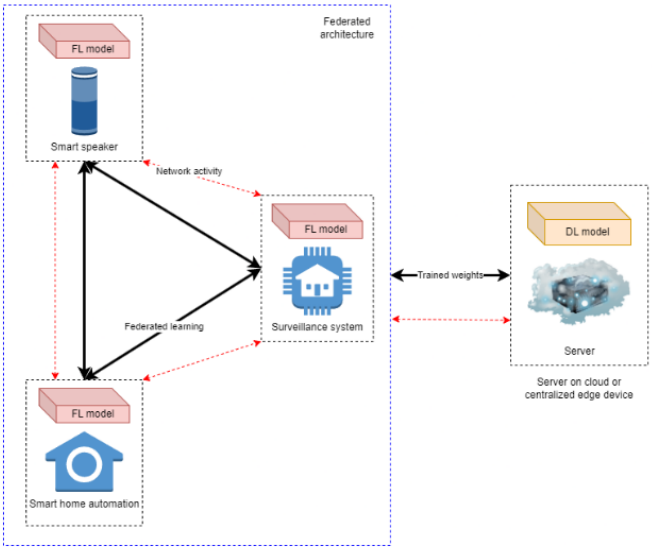

Figure 1.1: Federated architecture system diagram

The Python Pandas library is employed to convert CSV data into frames for data exploration and preparation. The core function focuses on training and evaluating machine learning models using raw data. This process involves removing irrelevant modeling columns and categorizing data as "benign" or "abnormal" to support supervised learning. An essential step involves partitioning benign data into subsets for training, threshold calculation, and model evaluation. During preprocessing, data elements are combined, reordered, and selected to introduce randomness.

The Scikit-learn StandardScaler is used to standardize training and test data. PyTorch tensors are obtained for either CPU or GPU processing. The configuration of hyperparameters and settings for federated learning involves nine clients participating, with variable client numbers in each communication round. Each iteration includes random client selection for training or model aggregation, with five training epochs per iteration. This iterative process refines the global model, and hyperparameter settings dictate the number of clients, training duration, and global model update frequency, ensuring flexibility. Random sampling from each device's dataset, with replacement and shuffling, utilizes PyTorch to load selected training or evaluation data. Data loaders are structured in a dictionary, using device labels as keys. Federated learning relies on the server's aggregate function at its core. It updates the global model with contributions from decentralized clients, considering local models and data. Federated averaging calculates weighted parameter averages for the global model, influenced by the number of samples in clients' datasets.

Clients with larger datasets have a more significant impact on global model modifications. The PyTorch-based deep autoencoder model serves dual purposes: data reconstruction and dimensionality reduction. It employs hyperbolic tangent (Tanh) activation functions and progressive linear layers for efficient data compression and decompression, ultimately reducing data dimensionality.

3.2 QoS monitoring

The research harnesses Mininet, an open-source network simulator, to create, explore, and evaluate Software-Defined Networking (SDN) applications and topologies. This platform facilitates the generation of complex network configurations with switches, routers, hosts, and links. Mininet provides network component virtualization, reducing both hardware and operational costs, thereby enabling extensive network emulation on a single workstation. Ensuring precise emulation of network features, including packet forwarding, latency, and capacity, is crucial for realistic SDN solution testing. Mininet seamlessly integrates with SDN controllers, and for this research, the OpenDaylight Controller, an open-source modular SDN controller, is initiated on the Karaf framework. This is accessible through VMware Workstation, providing access to the DLUX web interface.

The controller oversees SDN infrastructure and offers a web-based DLUX interface for centralized network management. To assess Quality of Service (QoS) for the Internet of Things (IoT), the study simulates an IoT network within the SDN topology. IoT devices are represented as hosts (e.g., h1-h8) with unique IP addresses ('10.0.0.x'). VideoLAN Client (VLC) streaming is used to replicate IoT data transmission, with one host typically serving as the VLC streaming server, while others act as IoT device clients. VLC streaming facilitates QoS evaluations, including bandwidth, jitter, and throughput, across IoT devices, enabling comprehensive network performance and QoS assessment within IoT contexts.

The study extends its focus to incorporate QoS monitoring into the SDN environment, enhancing real-time network analysis. A web-based dashboard, built using the Flask framework, empowers users to monitor network metrics like bandwidth, jitter, and throughput. Flask, combined with AJAX, facilitates dynamic interaction and real-time updates, allowing users to select specific tabs on the dashboard, triggering AJAX calls to fetch relevant data. Flask's validation mechanisms ensure the integrity of user inputs. The dashboard provides functionalities such as video streaming initiation, diagnostics, and real-time QoS monitoring, with Bwm-ng, a bandwidth monitoring tool, collecting data on bandwidth utilization, and presenting it in real-time through the dashboard.

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 170-176, November-2023
https://doi.org/10.47001/IRJIET/2023.711024

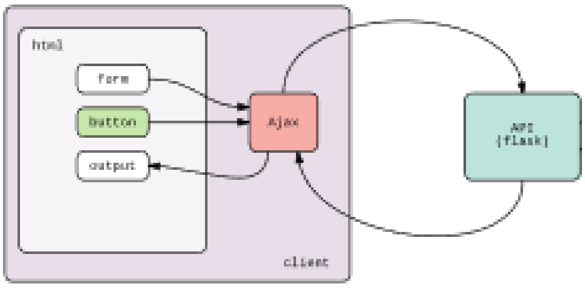

Figure 1.2: Integration of Ajax and Flask API

This study emphasizes the importance of understanding network traffic through tools like tcpdump and Wireshark. These tools help capture and analyze various traffic types, such as Web Traffic (HTTP, HTTPS), Streaming Traffic (RTMP, RTP), File Transfer Traffic (FTP, SCP), Database Traffic (SQL), Control Traffic (SDN, network administration), and Miscellaneous Traffic (ICMP, DNS).

3.3 Priority-based dynamic resource allocation

This study aims to investigate bandwidth allocation and Quality of Service (QoS) in networks employing Software-Defined Networking (SDN) and Internet of Things (IoT) technologies. The primary goal is to assign a significant portion of the available bandwidth to a specific host, denoted as "h1," while reducing bandwidth for other hosts. This approach prioritizes "h1." The research methodology involves crafting a custom Mininet network topology, where "h1" receives top priority and most of the available bandwidth, while other hosts get reduced bandwidth. This is achieved by configuring traffic management settings in the Mininet environment. The research framework enables the creation of tailored network topologies, the implementation of QoS rules, and experimentation with traffic prioritization. It commences with establishing a unique network topology, labeled "CustomTopology," consisting of eight hosts (h1 to h8) and eight switches (s1 to s8). Each host is assigned a unique IP and MAC address to simulate IoT devices. The TCLink class is used to configure specific bandwidth capacities for network links. The strategy involves using the "Increase_Bandwidth" function to adjust bandwidth allocation, giving precedence to "h1." This function reduces available bandwidth for other hosts while increasing it for "h1." The "configure_qos_policy" function constructs QoS policies for the high-priority host, involving the specification of a Differentiated Services Code Point (DSCP) value and applying bandwidth limits, relying on the OpenDaylight controller. The network architecture is instantiated in the main function using Mininet, including a RemoteController for communication with the SDN controller. The "configure_qos_policy" function receives input parameters, including the OpenDaylight controller's IP address, the switch's Data Path ID (DPID), and the host's MAC address.

3.4 AES in MQTT protocol

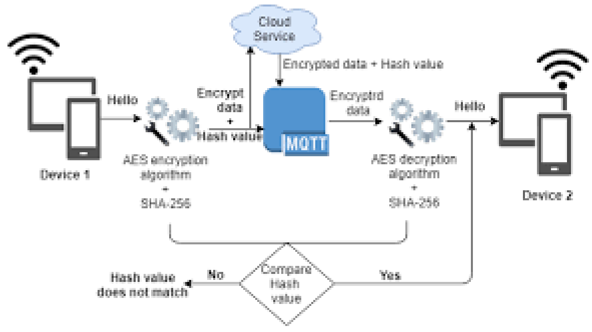
Cloud Service
Encrypted data + Hash value
Hello
Encrypt data + Hash value
MQTT
Encryptrd data
Hello
Device 1
AES encryption algorithm + SHA-256
AES decryption algorithm + SHA-256
Device 2
Hash value does not match
No
Compare Hash value
Yes

Figure 1.3: AES integration with MQTT protocol

The study employed a rigorous and systematic approach to enhance the security of the MQTT (Message Queuing Telemetry Transport) protocol. This methodological framework comprised a series of interrelated stages, each tailored to achieve specific research objectives. As visually represented in Figure 1.3, the structured methodology illustrated the integration of security components into MQTT, enhancing the overall clarity of the research process. The primary aim of this study was to improve the security and reliability of MQTT within Internet of Things (IoT) ecosystems through a methodical and well-defined approach. The research commenced with a comprehensive examination of the existing security measures within the MQTT protocol, with the goal of identifying vulnerabilities, constraints, and areas in need of enhancement. This assessment informed the formulation of precise research objectives, covering aspects such as data confidentiality, integrity, authentication, and scalability. The study delved into load balancing strategies, aiming to efficiently distribute MQTT traffic across multiple brokers to ensure scalability. Particular attention was devoted to optimizing encryption procedures, reducing computational overhead, and minimizing memory consumption, especially for resource-constrained Internet of Things (IoT) devices. Performance testing under controlled conditions was conducted to evaluate the impact of encryption on MQTT efficiency, involving the systematic collection and analysis of performance metrics, including latency, throughput, and CPU usage.

IV. RESULTS AND DISCUSSIONS

Even after 5 epochs of training, federated deep learning with deep auto encoders in the intrusion detection system showed promising results. With a restricted dataset from 5 Internet of Things (IoT) devices, the loss metric converged to 1.5 in 1.25 training rounds. The model's ROC curve had an exceptional AUC value of 1.00, indicating its robust ability to distinguish between normal and intrusive network activity. The precision-recall curve had an AUC of 1.00, indicating a highly accurate intrusion detection system with a high true positive rate. The model performed well, classifying data with 99.851% accuracy. It reduced false positives and detected all intrusions with a precision of 0.999 and a recall of 1.000. The F1 score was 99.921, indicating precision-recall equilibrium. True Positive Rate (TPR) was 0.99986, but False Positive Rate (FPR) was 0.02282, indicating a significant decrease in false alarms. Both the Receiver Operating Characteristic Area Under the Curve (ROC-AUC) and Average Precision metrics scored 1.000, indicating excellent intrusion detection performance.

The bandwidth monitoring experiment evaluated network performance during video streaming between hosts h1 and h5. The experiment focused on Ethernet Port 0 data transfer rates. H1, the originating entity, transferred data well, while H5 received and processed the stream. This statement highlights a robust QoS framework that manages high-bandwidth applications like video streaming across the network. In the jitter experiment, a server and client transferred 1.05 Mbits/sec over 10.016 seconds. A modest jitter of 0.004ms indicated a stable data transmission. The network was reliable because data packets were lost 0% of the time. In a server-client throughput experiment, 350 Mbits/sec was achieved in 10.0861 seconds. This study shows the network's efficacy, dependability, and ability to deliver high-speed data using TCP.

The third component shows that a dynamic and priority-based bandwidth allocation for QoS works. Host h1 receives an unfair bandwidth allocation, giving it more bandwidth than other hosts. This strategy prioritizes network h1 traffic. In conclusion, the project successfully dynamically allocates bandwidth by priority in the SDN IoT network. Preferential treatment gives host h1 a larger bandwidth share, improving its QoS. The presented method shows how SDN systems can implement effective bandwidth control mechanisms.

AES encryption gave MQTT a slight computational boost and 2ms longer message transmission and reception. This makes it suitable for low-latency IoT applications. A minimal 5-kilobyte (KB) increase in memory consumption and CPU usage below 3% during encryption and decryption showed efficient computing resource use. Encrypted communication dropped 3% to 150 messages per second (MPS) from 155 MPS. AES encryption protected against brute force and dictionary attacks. Thus, message confidentiality was maintained during testing.

IV. CONCLUSION

In conclusion, our research addresses the evolving needs of SDN-based IoT networks by enhancing QoS and security. Our approach integrates federated deep learning-based intrusion detection, real-time QoS monitoring, dynamic resource allocation, and improved MQTT AES encryption. The intrusion detection system, employing federated deep learning with deep autoencoders, showed swift convergence and excellent performance in accurately detecting malicious network traffic. Our experiments in bandwidth monitoring, jitter assessment, and throughput evaluation demonstrated the network's resilience, efficiency in handling high-bandwidth applications, stability, and rapid data transmission. The dynamic and priority-based bandwidth allocation highlighted our system's adaptability. AES encryption's minimal computational burden suits IoT applications with low latency needs, effectively utilizing computational resources, ensuring data confidentiality, and protecting against potential intrusions. Future research should focus on investigating the scalability and practical application of our proposed framework in the context of large-scale SDN-based IoT networks. This would necessitate assessing the efficacy of the framework in relation to the expansion of the network, as it adapts to a growing multitude of IoT devices and a wide range of applications. Furthermore, it is necessary to conduct additional research in order to evaluate the ability of our intrusion detection system to adapt to evolving threat environments. An additional area of investigation may entail the enhancement of our dynamic bandwidth allocation strategy, taking into account the balancing of device priority and resource utilization within fluctuating network circumstances. Furthermore, it would be advantageous to conduct an analysis of the framework's compatibility with various IoT standards and communication protocols, thereby expanding its potential for use in different contexts.

ACKNOWLEDGEMENT

We express our heartfelt gratitude to the Department of Computer Systems Engineering faculty for their guidance and expertise. We are particularly thankful to our supervisor, Ms. Hansika Mahaadikara, and co-supervisor, Ms. Dinithi Pandithage, for their unwavering support. Our sincere thanks also go to all contributors within the academic community for their encouragement and assistance in completing this research. Your support has been truly invaluable.

REFERENCES

[1] H. Moni Sree, R. Pavithra, R. B. Nithyaa Shri, and M. Shanthi, “Review on Iot Security and Its Real-Time Application,” 2021 International Conference on Advancements in Electrical, Electronics,

Communication, Computing and Automation, ICAECA, 2021.

[2] A.Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, “CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques,” 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019, May 2019.

[3] K. Sharma and R. Nandal, “A literature study on machine learning fusion with IoT,” Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019, vol. 2019-April, pp. 1440–1445, Apr. 2019.

[4] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, “ToN_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets,” IEEE Internet Things J, vol. 9, no. 1, pp. 485–496, Jan. 2022.

[5] K. H. Manguri and S. M. Omer, “SDN for IoT Environment: A Survey and Research Challenges,” ITM Web of Conferences, vol. 42, p. 01005, 2022.

[6] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, “Complementing IoT Services through Software Defined Networking and Edge Computing: A Comprehensive Survey,” IEEE Communications Surveys and Tutorials, vol. 22, no. 3, pp. 1761–1804, Jul. 2020.

[7] A.Dvornikov, P. Abramov, S. Efremov, and L. Voskov, “QoS Metrics Measurement in Long Range IoT Networks,” Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017, vol. 2, pp. 15–20, Aug. 2017.

[8] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban, and N. D. Han, “A Survey of QoS-aware Routing Protocols for the MANET-WSN Convergence Scenarios in IoT Networks,” Wirel Pers Commun, vol. 120, no. 1, pp. 49–62, Sep. 2021.

[9] V. Gugueoth, S. Safavat, and S. Shetty, “Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects,” ICT Express, Mar. 2023.

[10] S. Niknam, H. S. Dhillon, and J. H. Reed, “Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges,” IEEE Communications Magazine, vol. 58, no. 6, pp. 46–51, Jun. 2020.

[11] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, “A survey on security and privacy of federated learning,” Future Generation Computer Systems, vol. 115, pp. 619–640, Feb. 2021.

[12] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, “Federated Wireless Network Intrusion Detection,” Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019, pp. 6004–6006, Dec. 2019.

[13] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A. R. Sadeghi, “DÏoT: A federated self-learning anomaly detection system for IoT,” Proc Int Conf Distrib Comput Syst, vol. 2019-July, pp. 756–767, Jul. 2019.

[14] D. Attota, V. Mothukuri, R. Parizi, S. P.-I. Access, and undefined 2021, “An ensemble multi-view federated learning intrusion detection for IoT,” ieeexplore.ieee.org, Accessed: May 03, 2023.

[15] O. Friha, M. Ferrag, L. Shu, … L. M.-J. of P. and, and undefined 2022, “FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things,” Elsevier, Accessed: May 03, 2023.

[16] Y. Zhao, J. Chen, D. Wu, J. Teng, and S. Yu, “Multi-task network anomaly detection using federated learning,” ACM International Conference Proceeding Series, pp. 273–279, Dec. 2019.

[17] Z. Lian and C. Su, “Decentralized Federated Learning for Internet of Things Anomaly Detection,” ASIA CCS 2022 - Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security, pp. 1249–1251, May 2022.

[18] A.Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Communications Surveys and Tutorials, vol. 17, no. 4, pp. 2347–2376, Oct. 2015.

[19] B. K. Mukherjee, S. I. Pappu, M. J. Islam, and U. K. Acharjee, “An SDN based distributed IoT network with NFV implementation for smart cities,” Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, vol. 325 LNICST, pp. 539–552, 2020.

[20] J. R. Naif, G. H. Abdul-Majeed, and A. K. Farhan, “Secure IOT System Based on Chaos-Modified Lightweight AES,” 2019 International Conference on Advanced Science and Engineering, ICOASE 2019, pp. 12–17, Apr. 2019.

[21] F. Dewanta, B. Y. Yustiarini, B. Indrakusumo, and R. Harsritanto, “A study of secure communication scheme in MQTT: TLS vs AES cryptography,” JURNAL INFOTEL, vol. 14, no. 4, pp. 269–276, Nov. 2022.

[22] J. Ahamed, M. Zahid, M. Omar, and K. Ahmad, “AES and MQTT based security system in the internet of things,” Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 8, pp. 1589–1598, Nov. 2019.

[23] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," 2021 International Conference on Computer System, Information Technology, and Electrical Engineering, COSITE 2021, pp. 166–170, 2021.

[24] C. Okur, A. Orman, and M. Dener, "DDOS Intrusion Detection with Machine Learning Models: N-BaIoT Data Set," pp. 607–619, 2022.

[25] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep Learning for Anomaly Detection," ACM Computing Surveys (CSUR), vol. 54, no. 2, Mar. 2021.

[26] G. D'Angelo and F. Palmieri, "Network traffic classification using deep convolutional recurrent auto encoder neural networks for spatial–temporal features extraction," Journal of Network and Computer Applications, vol. 173, Jan. 2021.

Citation of this Article:

Sathiamoorthy A., Mithusan S., Rathnayaka R.M.L.R., Kajenthiran S., Mahaadikara M.D.J.T. Hansika, Dinithi Pandithage, "StreamSafe: Improving QoS and Security in IoT Networks" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 170-176, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711024

****