International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Secure Data Transmission in Wireless Fog Networks through Software-Defined Networking Solutions

Deepthi Kothapeta[1], Madiraju Jagadeeshwar[2]

Submitted: 30/12/2023 **Revised**: 06/02/2024 **Accepted**: 14/02/2024

Abstract: The centralised control intelligence in the next-generation networking architecture of Software-Defined Networks (SDN) is what gives them their strength. SDN's control plane can be extended to a variety of underlying networks, including fog and the Internet of Things (IoT). Real-time data management is currently possible with the fog-to-IoT architecture. However, most fog-to-IoT devices are geographically dispersed and have limited resources, which leaves them open to cyber attacks. Recently, a unique cyber foraging approach has emerged to shift heavy workloads from mobile devices to mobile cloudlets situated close to end users. Because wireless one-hop communication is common near the network edge, wireless mesh networks(WMNs) are being investigated as a potential solution for developing wireless fog networks. On the other hand, the global network administration and monitoring capabilities that fog networks require are limited by the distributed hop-by-hop routing protocols that WMNs utilize to depict apartial picture of the network. SDN is a great fit for fog-based communication systems since it enables centralized control and management of the entire network. The SDN Open Flow protocol is primarily meant for wired networks hence, it doesn't enable wireless fog networks. This paper proposes a novel trust-based identity model for the Internet of Things architecture for handling fog networks (TbI-IoT-FN) to provide safe data transmission in the network, combining the benefits of fog computing and software-defined networking. In software-defined networking, sophisticated algorithms for resource management and traffic control can be implemented thanks to a logically centralized network control plane. When comparing the suggested model to the current model, the findings show that the proposed model performs at a higher level.

Keywords*: Software Defined Network, Wireless Fog Networks, Secure Data Transmission, Routing Protocol, Trust Identity.*

1. Introduction

Fog Computing extends cloud computing capabilities to edge networks, improving latency and reliability. It relies on forward-deployed servers in proximity to mobile devices [2] for tasks like data collection and processing offloading. Despite its benefits, public Wi-Fi hotspots in fog-networks face capacity challenges due to unpredictable network capacity [1].

Given cloud computing's significant role in data storage, fog computing aims to minimize delays between nodes, crucial for delay-sensitive applications. The development of an SDN-based fog seeks to facilitate node-to node communication, ensuring optimal performance[4]. This discussion presents the latest state-of-the-art research on SDN-fog computing, with a specific focus on addressing network performance issues.

In SDN-based smart grids, employing a three-tiered architecture with fog, IoT, and cloud tiers simplifies data transmission complexities [5]. SDN controllers in the bottom tiers manage cloud processing and storage, while the top cloud tier handles permanent storage. The Dijkstra Algorithm utilizes three path recovery types for shortest paths during link breakdowns [7]. Results indicate that the proposed middleware, managing application heterogeneity, can efficiently select the best forwarding method based on the application type and network state [10][11].

SDN offers significant advantages in addressing networking challenges by separating data and control layers, providing flexibility in network configuration[12][13]. The control layer, acting as the network's brain, houses the primary controller, determining routing, while the application layer handles network or commercial applications. The data plane includes cyber-physical components, and SDN's global network view enhances flexibility, and orchestration, and reduces logistical efforts. Its application extends to complex technologies like cyber-physical systems, ensuring reliable network management and contributing to strengthened network resilience. SDN brings benefits such as improved network visibility, enhanced device utilization and seamless service integration [13].

The integration of machine learning in computer networks holds promise for enhancing resilience [15]. Centralizing the network controller in application networking enables the application of machine learning to cyber-physical systems [16]. This capability enhances resilience through optimized traffic forwarding decisions and adaptive routing policies based on network data.

[1] *Research Scholar, Dept. of Computer Science, Chaitanya Deemed to be University,*
deepthivaishu18@gmail.com

[2] *Professor, Dept. of Computer Science, Chaitanya Deemed to be University*
jagadeeshwar07@gmail.com

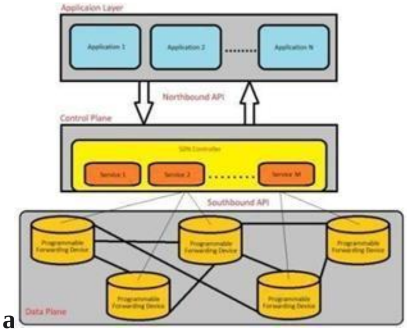
Application Layer
Application 1
Application 2
Application N
Northbound API
Control Plane
SDN Controller
Service 1
Service 2
Service M
Southbound API
Programmable Forwarding Device
Programmable Forwarding Device
Programmable Forwarding Device
Programmable Forwarding Device
Programmable Forwarding Device
Data Plane
a

Fig 1: A generic model of the SDN architecture

The foundation of SDN emphasizes the centralized control of the entire network by a single control unit, moving away from managing individual network devices. Cloud computing introduce sun resolved questions in networking mobility, scalability, and security, while also creating opportunities for expanding application networks [17]. Fog computing, facilitating IoT applications with lower latency and increased bandwidth, introduces diversity and challenges for end devices with limited resources. Addressing these challenges involves extending SDN benefits to cloud and fog computing [18].

Resource management issues, such as capacity heterogeneity, asymmetrical communication, uneven workloads, and resource dependence, pose challenges [19]. This study explores the advantages of SDN-based cloud computing for energy savings and network performance, focusing on fog computing and software-defined networks [20]. SDN cloud and SDN fog are identified as promising areas, and researchers assess their relative significance. The work serves as a valuable reference for infrastructure cloud/fog by categorizing fresh data and analyzing it based on various criteria [21]. Each reviewed study is mapped using pertinent metrics to facilitate the grouping of related studies.

The research aims to provide a lightweight, secure, and energy-efficient routing system using a fog-based protocol for limit-sensing networks with secure data transmissions [22]. Additional security measures prevent unauthorized access to sensor data [23]. A dynamic distance threshold reduces transmission costs, leading to lower over head and less frequent sharing of local information among sensor nodes, consuming less unnecessary energy [24]. QoS settings are considered for data transportation between fog nodes and cloud servers or between cluster heads and the fog layer. A packet delay parameter enhances system performance in data transmission and route management [25]. The second level of security implements a robust asymmetrical encryption mechanism between fog nodes and cloud servers, ensuring data protection from cluster heads to fog nodes [2].

2. Literature Survey

In the realm of distributed learning techniques, challenges emerge from the absence of a centralized controller, posing potential threats to system stability. Despite advancements in deep neural networks for attack detection, concerns persist regarding the lack of a centralized approach for cost mitigation in fog nodes [2] [4]. Fog-IoT intrusion detection, employing diverse machine-learning techniques, grapples with vulnerabilities in the absence of a central controller [5].

A foundation for ongoing study is laid out by resilience principles outlined in[7], addressing organizational and physical architectural resilience in network design.[10] proposes an innovative approach to the robust controller positioning problem, enhancing control plane robustness by considering switch needs and controller capabilities. [12] suggests a novel architecture integrating nodes and links with SDN to fortify network resilience. The incorporation of machine learning within SDN models contributes to improving attack identification and intrusion detection system robustness, as proposed by [15].

The methodology put forth by [16] tackles QoS routing in delay-restricted cyber-physical robotic systems, dynamically creating efficient QoS techniques with minimal overhead.[17] provides a comprehensive overview of applying machine learning to security, introducing a threat taxonomy. The emergence of machine learning within the SDN model for resilience allows for flexibility within certain limits, as evidenced by [19] [20] [21].

Proposed AES algorithm encryption for fog nodes by[19],a long side the efficacy of deep- learning in identifying malware threats, showcases promising results. [20] addresses the failure rate of traffic entering the SDN controller through machine learning methods. The DNN approach suggested by [22], while lacking a centralized controller for anomaly identification, underscores the need for further investigation into comparing deep learning and machine learning algorithms [23].

Fog computing plays a pivotal role in detecting attacks on

IoT devices, with fuzzy techniques achieving over 80% accuracy, as highlighted by [24]. The proposed method in [25] efficiently identifies nodes infected with a virus in an IoT ecosystem, managing computation overhead effectively. The integration of SDN and fog nodes enhances network capabilities, offering real-time analytics and calculations at the network's edge, as demonstrated by [26].

3. Proposed Model

SDN has garnered significant attention across various domains, including research networks, data centers, and wired provider networks. Its innovative approach, separating control and data planes, reduces protocol rigidity and enables adaptable behavior. Unlike traditional IP networks, SDN relies on flows instead of packets for forwarding, with centralized network management facilitating rapid innovation and administration. This paper explores SDN implementation in wireless networks, emphasizing its application in data centers, virtualization, residential networking, security, and the Internet of Things (IoT).

Numerous solutions have emerged around the SDN concept, with architectures designed for horizontal IoT systems. However, some proposals neglect coordinated cloud computing and secure mobility challenges. An illustrated architecture of an SDN-enabled wireless fog network is presented in Figure 2. The script utilizes shortest pathways to optimize routing for packets from various fog routers, employing real-time monitoring and traffic engineering for efficient traffic redirection.

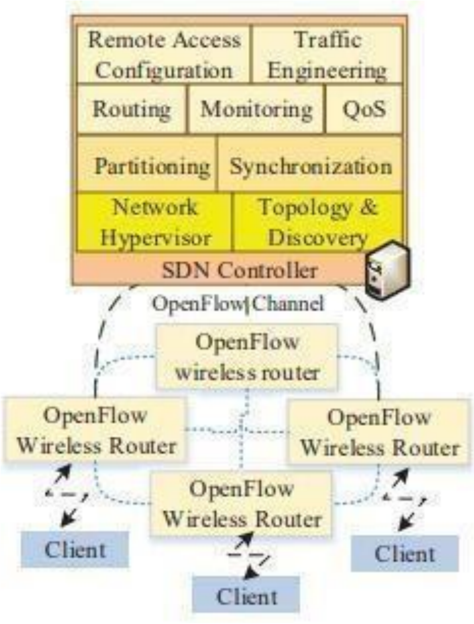

Fig 2 : Architecture of the SDN-enabled Wireless Fog Network

Integrating Wireless Sensor Networks (WSN) with fog computing capabilities enables diverse network operations, addressing challenges posed by limited sensor node resources. The proposed fog-based power routing protocol enhances data collection, storage, and processing efficiency while minimizing$^{i=}$e^{1}nergy consumption and network latency. The algorithm introduces the trust-based identity model (TbI-IoT-FN), specifically tailored for the Internet of Things architecture, addressing intricacies in fog networks and ensuring secure data transfer.

```
AlgorithmTbI-IoT-FN
{
Input:NodesinNetwork
Output:TrustedRouteforSecureDataTransmission
Step1: To provide safe data transmission, the SDN network is setup. Every node within the network is
```

registered to verify their identification. The node data gathering is carried out as

$$\boldsymbol{Nreg[k]=\sum_{i=1}^{L} H(Node(i))+R+Th}$$

$$\boldsymbol{Nodedata[k]=\sum^{L} S(Node(i))+r(Msg)+Nreg(i)}$$

Here R is the time of the node entry, this is the threshold value, τ is the total packets in a message Msg.

Step2: Each registered node is designated as a trustworthy node to participate in data transmission by generating a trust factor for each node. Calculating the trust factor is done as follows:

$$Tr = Nreg(i) + \left(\frac{allocener(Nreg(i))L}{availener(Nreg(i))} + \tau \right)$$

$$Tf\,(Nreg(i)) = \sum_{i=1}^{L} \max(Tr) + \max comp(Nreg(i)) + Th + \frac{nodes(Nreg(i))}{\tau}$$

Step 3: The SDN network is configured to take the network path into account. To ensure safe data transmission, the route identification process is carried out to include the majority of trusted nodes in the routing process. The routing is carried out as follows:

Here λ is the maximum available energy node and ω is the total users in the system

$$Rout[V] = \max\left(\lambda + Tr * \left(\frac{Tf(Nreg(i))}{\omega}\right) + \left(\frac{Tf(Nreg(i+1))}{\omega}\right)\right)$$

Step 4:To enhance network performance, malicious nodes are identified in the SDN network. The detection of malicious nodes is carried out as

$$MalS[M] = \sum_{i=1} minPDR(Nreg(i)) + minener(Nreg(i)) + maxLoad(Nreg(i))$$

Step 5:To execute the improvement in data transmission levels, the network's data loss rate is determined. In fog networks, the data loss rate is computed as

$$\underline{Dloss}(Nreg(i))$$

$$= min(r(Nreg(i)) + Tf(Nreg(i))$$

$$-sim(PDR(Nreg(i),PDR(Nreg(i+1)))$$

Results

The edge of the network plays a crucial role in processing IoT-generated data, as devices constantly collect, store, transmit, and process data in an IoT-driven environment. Analyzing this data provides valuable insights for better decision-making. Fog computing is transforming data storage and processing by bringing cloud-like capabilities closer to end users. Fog/edge servers, resembling thin-client cloud servers, are strategically deployed near end users in fog/edge computing systems. These servers offer high-quality services for instant processing of IoT data, including storage, computation, analysis, and processing.

The proposed model, implemented in Java using the Cloud Sims package and executed in Eclipse, introduces the Trust-Based Identity model for the Internet of Things architecture designed for managing fog networks (TbI - IoT-FN). This model is compared with the standard Software-Defined Network-Enabled Fog-to-Things Hybrid Deep Learning-Driven Cyber Threat Detection System (SDN-FIoT-HDL).

In the proposed model, nodes requiring data transmission register with the cloud service provider. The cloud service provider maintains all user data in the cloud setup, utilizing it for future validations and authentications. The node registration accuracy of the proposed model surpasses that of the current model, as illustrated in Figure 3, transparently showcasing the improved levels of node registration accuracy.

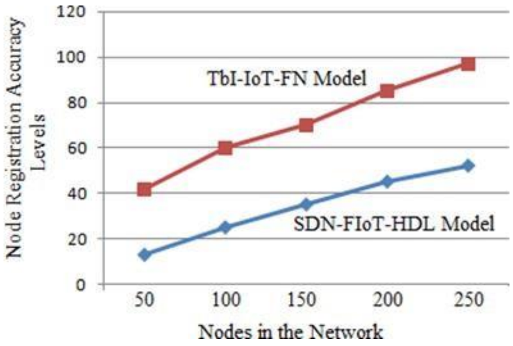

Fig 3: Node Registration Accuracy Levels

Nodes, in the context of fog computing, represent distributed entities with processing and sensing capabilities. These entities consist of one or more connected devices and play a crucial role in implementing fog services. Fog computing enhances service quality by accelerating response times, minimizing transmission latency and traffic, and enabling bandwidth savings.

To ensure optimal operation, only trusted fog nodes are considered, emphasizing the importance of reliability in the fog computing environment. Figure 4 illustrates the computation accuracy of the fog node trust level, providing insights into the trustworthiness of these nodes.

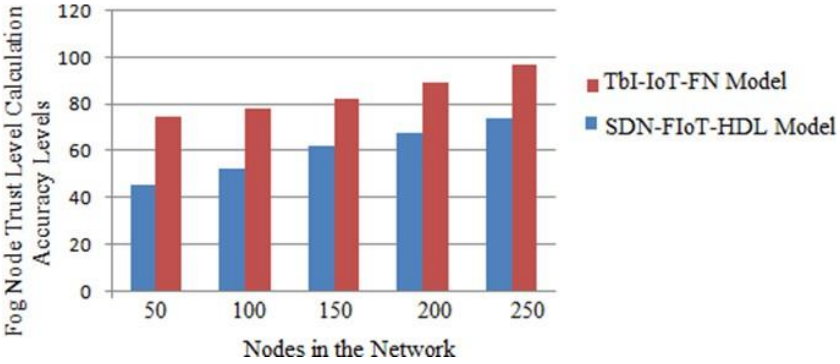

Fig 4: Fog Node Trust Level Calculation Accuracy Levels

In digital communications, there is a possibility that one or more sent data packets may not reach their intended destination. This scenario can result in data transmission loss, leading to observable performance issues in various forms of digital communication.

A data packet, in this context, refers to a brief piece of information transmitted through a network protocol in a packet-switched network, such as the Internet. Network packets typically contain information such as sender and recipient addresses, protocols, and IDs. Various online activities, including messaging and video downloads, rely on the successful transmission of packets.

Figure 5 illustrates the data transmission loss rate, providing a visual representation of the extent to which data packets may be lost during transmission.

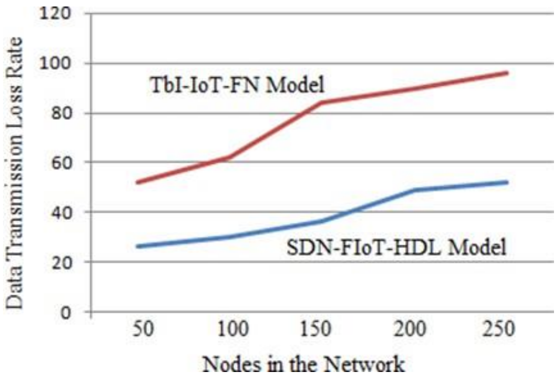

Fig 5: Data Transmission Loss Rate

Software-defined networking (SDN) is a networking technique that employs software-based controllers or APIs to control network traffic and interact with the underlying hardware resources. It is an architectural concept that enables network programming, allowing network managers to oversee the entire network, irrespective of the specific network technology in use.

In the context of the current discussion, Figure 6 illustrates the SDN network data transmission rate for both the suggested model and the existing model. This visual representation provides insights in to how SDN influences the rate at which data is transmitted across the network in comparison to the proposed and current model.

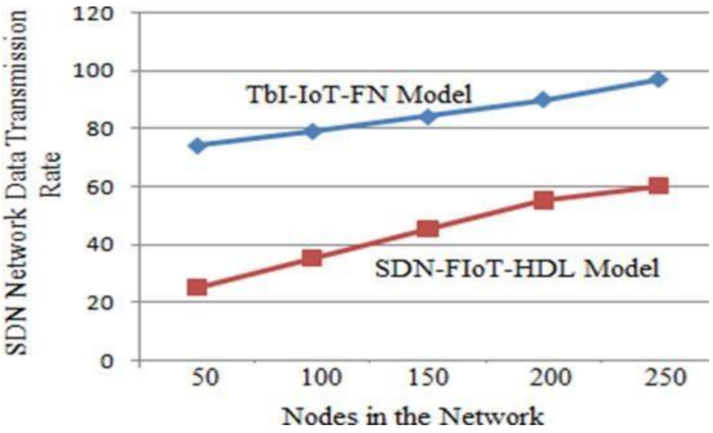

Fig 6: SDN Network Data Transmission Rate

The SDN concept aims to shift control of network routing from individual network devices to a centralized control layer. This change introduces new methods for planning, constructing, and managing networks. Routing, the process of selecting a path for traffic within or across networks, becomes a crucial aspect in this context. This concept of routing is widely applicable across various types of networks, particularly in circuit-switching networks.

.

As depicted in Figure7, the levels of SDN routed etection time are presented. This visual representation helps in understanding the time dynamics associated with route detection in an SDN-enabled network, offering insights into the efficiency and speed of the routing process

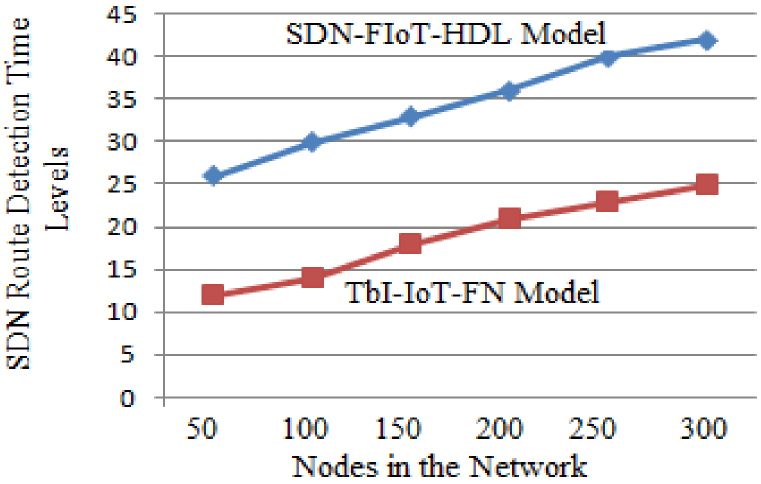

Fig 7:SDN Route Detection Time Levels

4. Conclusion

By employing a centralized control mechanism facilitated by an SDN controller, the recommended detection method aims to reduce computational load. The integration of IoT sensors and WSNs in recent years has contributed to achieving high-speed routing for network users. However, the constrained resources of sensor nodes pose optimization challenges for network longevity and data security in both industrial and academic applications. This study proposes a fog-based routing protocol for constraint sensors, strategically selecting cluster heads with minimal transmission overhead while prioritizing safety and energy efficiency. The protocol incorporates dynamic thresholds with multiple parameters and utilizes multi-faceted QoS criteria to determine the next hop from the observation region to the fog layer, minimizing energy consumption and delay rate.

The protocol results in a reduction in packet delivery ratio, data delay, and communication overhead. The integration of these protocols establishes an SDN-enabled method for managing wireless fog networks, incorporating a trust-based identity model for the Internet of Things architecture. The proposed approach offers an adaptable wireless data plane and adaptive traffic engineering to alleviate network stress in fog networks.

Performance evaluation demonstrates the effectiveness of their commended strategy, showcasing lower-latency communication, flexible load balancing for optimal shortest path selection, and reduced network overhead. Future work will focus on integrating SDN radio resource management and network resource management to enhance spectrum consumption and address channel interactions through a cross-layer architecture compatible with SDN. Additionally, considerations for distributed attacks will be crucial in determining security levels in future implementations.

References

[1] Arif, Muhammad, Ullah, Ihtisham, Raza, Basit,Ali, Sikandar, Abbasi, Irshad Ahmed, Baseer, Samad Irshad, Azeem, 2021, Software Defined Network Enabled Fog-to-Things Hybrid Deep Learning Driven Cyber Threat Detection System,1939-0114, https://doi.org/10.1155/2021/6136670, 10.1155/2021/613667.

[2] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, “A new framework for DDoS attack detection and defense in SDN environment,” IEEE Access, vol. 8, Article ID 161919, 2020. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9186014

[3] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, “Machine learning algorithms to detect DDoS attacks in SDN,” Concurrency and Computation: Practice and Experience, vol. 32, no. 1, Article ID e5402, 2020. https://doi.org/10.1002/cpe.5402

[4] .Galeano,J.M.Carmona,J.F.V.Valenzuela,andF.V.L una,"Detection and mitigation of dos and ddos attacks in iot-based stateful sdn: an experimental approach," Sensors, vol. 20, no. 3, 2020. https://doi.org/10.3390/s20030816

[5] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765

[6] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in Proceedings of the IEEE 1st International Workshops on Foundations and Applications of Self∗Systems (FAS∗W), IEEE, Augsburg, Germany, September 2016. https://ieeexplore.ieee.org/document/7789475

[7] S. Ali, V. Kumar, A. A. Laghari, S. Karim, and A. B. Anwar, "Comparison of fog computing & cloud computing," International Journal of Mathematics and Soft Computing, vol. 5, no. 1, pp. 31–41, 2019.

[8] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues," The Journal of China Universities of Posts and Telecommunications, vol. 23, no. 2, pp. 56 – 96, 2016.

[9] S. Ivanov, S. Balasubramaniam, D. Botvich, and O. B. Akan, "Gravity gradient routing for information delivery in fog wireless sensor networks," Ad Hoc Networks, vol. 46, pp. 61 – 74, 2016.

[10] Ku, Y. Lu, and M. Gerla, "Software-defined mobile cloud: Architecture, services and use cases," in International Wireless Communications and Mobile Computing Conference, IWCMC 2014, Nicosia, Cyprus, August 4-8, 2014, 2014, pp. 1–6.

[11] K. Liang, L. Zhao, X.Chu, and H.H.Chen, "An integrated architecture for software defined and virtualized radio access networks with fog computing," IEEE Network, vol. 31, no. 1, pp. 80–87, 2017.

[12] X. Sun and N. Ansari, "Edgeiot: Mobile edge computing for the internet of things," IEEE Communications Magazine, vol. 54, no. 12, pp. 22–29, 2016.

[13] X. He, Z. Ren, C. Shi, and J. Fang, "A novel load balancing strategy of software-defined cloud/fog networking in the internet of vehicles, "China Communications, vol. 13, no. Supplement2, pp. 140–149, 2016.

[14] S. A. Lazar and C. E. Stefan ,"Futurevehicularnetworks:Whatcontroltechnologies?"in2016International Conference on Communications (COMM), 2016, pp. 337–340.

[15] Y. Xu, V. Mahendran, and S. Radhakrishnan," Towards sdn-based fog computing: Mqttbroker virtualization for effective and reliable delivery," in 2016 8th International Conference on Communication Systems and Networks (COMSNETS), 2016, pp. 1–6.

[16] R. Bruschi, P. Lago, G. Lamanna, C. Lombardo, and S. Mangialardi, "Openvolcano: An open- source software platform for fog computing," in 2016 28th International Teletraffic Congress (ITC 28), vol. 02, 2016, pp.22–27.

[17] Betzler, F. Quer, D. Camps-Mur, I. Demirkol, and E. Garcia- Villegas, "On the benefits of wireless sdnin networks of constrained edge devices," in 2016 European Conference on Networks and Communications (Eu CNC), 2016, pp. 37–41.

[18] L. Huang, G. Li, J. Wu, L. Li, J. Li, and R. Morello," Software-defined qos provisioning for fog computing advanced wireless sensor networks," in 2016 IEEE SENSORS, 2016, pp. 1–3.

[19] Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," IEEE Communications Magazine, vol. 56, no. 9, pp. 124–130, 2018.View at: Publisher Site| Google Scholar N. Chockwanich and V. Visoottiviseth, "Intrusion detection by deep learning with tensor flow," in Proceedingsofthe21stInterna- tionalConferenceonAdvanced Communication Technology (ICACT), IEEE Pyeong Chang, Korea(South),May2019.

[20] Samy, H. Yu, and H. Zhang, "Fog-based attack detection framework for internet of things using deep learning," IEEE Access, vol. 8, Article ID 74585, 2020.

[21] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," Simulation Modelling Practice and Theory, vol. 101, Article ID 102031, 2020.

[22] D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U.

Ghosh, and P. Sharma, “Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment,” Journal of Information Security and Applications, vol. 60, Article ID 102866, 2021.

[23] Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, “CA-secure ABE with outsourced decryption for fog computing,” Future Generation Computer Systems, vol. 78, pp. 730–738, 2018.

[24] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson’s Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[25] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In Healthcare Analytics, 2023, 4, 100219

[26] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(6s), pp. 720–729

[27] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges, 2023, pp. 305–321

[28] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(6s), pp. 765–774

[29] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023, 2023, pp. 1716–1721

[30] Vishwanath, R. Peruri, and J. H. Selena, Security in Fog Computing through Encryption, Digital Commons@ Kennesaw State University, Kennesaw, Georgia, USA, 2016.

[31] M. Ring, S. Wunderlich, D.Grüdl,D.Landes,andA.Hotho,“Flow-based benchmark datasets for intrusion detection,” in Proceedings of the 16th European Conference on Cyber Warfare and Security, pp.361–369,ACPI, Dublin, Ireland, June 2017.

[32] K. M. S. Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, “Preventive determination and avoidance of DDoS attack with SDN over the IoT networks,” in Proceedings of the 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0(ACMI),pp.1–6, IEEE, Rajshahi, Bangladesh,July2021.

[33] F.KHussain,W.Rahayu,andM.Takizawa,“Specialiss ueonintelligentfogandinternetofthings (IoT)-Based services,” World Wide Web, vol. 24, no. 3, pp. 925–927, 2021.

[34] S. Strecker, W. V. Haaften, and R.Dave,“Ananalysis of IoT cyber security driven by machine learning,”in Proceedings of the International Conference on Communication and Computational Technologies, pp. 725–753, Springer, Jaipur, India, February 2021.

[35] T. A. Tang, L. Mhamdi, D. McLernon, S. A. Raza Zaidi,and M.Ghogho,“Deep learning approach for network intrusion detection in software defined networking,” in Proceedings of the 2016 international conference on wireless networks and mobile communications (WINCOM), pp. 258–263, IEEE, Fez, Morocco, October 2016.

[36] Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” Ieee Access, vol. 5, pp. 21954–21961, 2017.

[37] F. Jiang, Y. Fu, B. B. Gupta et al., “Deep learning based multi-channel intelligent attack detection for data security,” IEEE transactions on Sustainable Computing, vol. 5, no. 2, pp. 204–212, 2018.

[38] Y. Xin, L. Kong, Z. Liuetal.,“Machine learning and deep learning methods for cyber security,”Ieee access, vol. 6, Article ID 35381, 2018.

[39] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, “Design of cognitive fog computing for intrusion detection in Internet of Things,” Journal of Communications and Networks, vol. 20, no. 3, pp. 291– 298, 2018.

[40] S. Rathore, J. H. Park, and H. P. Jong, “Semi-supervised learning based distributed attack detection framework for IoT,” Applied Soft

Computing, vol. 72, pp. 79–89, 2018.

[41] V. L. L. Thing, “IEEE 802.11 network anomaly detection and attack classification: a deep learning approach, “in Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC),pp.1–6, IEEE, San Francisco, CA, USA, May 2017.

[42] Q. Yaseen, M. Aldwairi, Y. Jararweh, M. A. Ayyoub, and B. Gupta, “Collusion attacks mitigation in internet of things: a fog based model,” Multimedia Tools and Applications, vol. 77, no. 14, pp. 18249–18268, 2018.

[43] C. Byers, “Architectural imperatives for fog computing: use cases, requirements, and architectural techniques for fog-enabled iot networks,” IEEE Communications Magazine, vol. 55, no. 8, pp. 14–20, 2017.

[44] Abeshu and N. Chilamkurti, “Deep learning: the frontier for distributed attack detection in fog-to-things computing,” IEEE Communications Magazine, vol. 56, no. 2, pp. 169–175, 2018.

[45] S. Khater, B. W. B. A. Wahab, M. Y. I. B. Idris, M. A. Hussain, and A. A. Ibrahim, “A lightweight perceptron-based intrusion detection system for fog computing,” Applied Sciences, vol. 9, no.1, 2019.

[46] O. E. Zaballa, D Franco, and M Aguado, “Next-generation SDN and fog computing: a new paradigm for SDN-based edge computing,” in Proceedings of the 2nd Workshop on Fog Computing and the IoT (Fog-IoT2020), Schloss Dags