Attack Detection in Internet of Things using Software Defined Network and Fuzzy Neural Network

Fahiba Farhin*, Ishrat Sultana*, Nahida Islam*, M Shamim Kaiser*, Md. Sazzadur Rahman* and Mufti Mahmud †
*Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh
†Department of Computing and Technology, Nottingham Trent University, NG11 8NS – Nottingham, UK
Email: {farhinfahiba, ishratshapno,nahida11.islam}@gmail.com, {mskaiser, sazzad}@juniv.edu
mufti.mahmud@ntu.ac.uk

***Abstract*—Internet of Things (IoT) is a dynamic and distributed wide network system that can integrate a gigantic number of pervasive sensors (i.e., physical objects), wireless nodes, and ubiquitous computing systems. These sensors can collect tons of raw data, send them to the internet at an unprecedented rate, and convert them to actionable insights using computing systems. These sensing nodes or physical objects are vulnerable and have upraised cybersecurity threats. In this work, we proposed the attack detection model for IoT using Software-defined network (SDN). The SDN controller can analyze the traffic flow, detect the anomaly, and block incoming traffic as well as the source nodes. In the SDN, a Fuzzy neural network (FNN) based attack detection system is considered which can detect attacks such as man-in-the-middle, distributed denial of service, side-channel, and malicious code. The FNN is trained and tested using NSL-KDD datasets. The evaluated performance exhibits that the FNN based attack detection system can detect the mentioned attack with an accuracy of 83%.**

***Index Terms*—IoT, SDN, Attack Detection, FNN, NSL-KDD Dataset**

I. Introduction

With the emergence of the smart pervasive sensors, the Internet of Things (IoT) is adopted in many applications such as smart city, environment monitoring, e-health, etc. Due to the increasing threats by cybercriminals, the security concern for IoT devices have raised. To date, no silver bullet has been confirmed which guarantees the shield for the IoT devices. In consequence, real-time monitoring and a decision support system for such IoT devices are essential [1].

Software-Defined Network (SDN) is a centralized system that divides data and control planes and is more suitable to ensure security measures of such systems. The SDN based IoT network can monitor the traffic behaviour in near real-time and detect attacks [2].

The nodes in the SDN-IoT system produce a gigantic volume of overhead control packets for the control plane which may increase power dissipation. The artificial intelligent agent /soft computing/brain-inspired techniques can assist such heterogeneous network to monitor traffic behaviour and detect the attack in the IoT system [3]. IoT-IDM is an intrusion detection and mitigation framework that imposes SDN with OpenFlow protocol and machine learning techniques for detecting known attacks in the smart home environments which works on learned signature patterns [4].

Abdolmaleki *et al.* [5] proposed Fuzzy Topology Discovery Protocol (FTDP) to enhance the overall performance of the software-defined wireless sensor networks. Alshehri *et al.* [6] offered a cluster-based fuzzy-logical approach where at first a fuzzy logic-based protocol is imposed that can determine various attacks and malicious nodes; secondly described maintenance of IoT nodes using this approach and thirdly, introduced a hexadecimal value-based firm message system for that IoT nodes like serial communication.

Mengmeng *et al.* [7] proposed deep learning-based a feed-forward neural network classifier for finding four categories of cyber-attacks in IoT networks, namely: Distributed Denial-of-Services (DDoS), Denial-of-Services(DoS), reconnaissance, and message theft. Improved genetic algorithm (GA) and deep belief network (DBN) based intrusion detection model is proposed in [8], [9]. Adaptively generated multiple neurons in an optimal number of hidden layers and different iterations of the GA used in detecting intrusion with a high accuracy rate experimented by NSL-KDD [10].

CBSigIDS is developed in [11] which is a blockchained signature-based intrusion detection system (IDS), works on a generic framework that can create and change database with trusted signature incrementally in a collaborative IoT network environment without a trusted intermediary.

Bhattacharjee *et al.* [12] evaluates data mining based model using two machine learning algorithms - K-Means and Fuzzy C-Means clustering algorithms to detect four vital attack categories i.e. (DoS), Remote to Local (R2L), User to Root (U2R) and Probe in NSL-KDD dataset.

So far researchers have detected four most common attacks such as DoS, Probe, R2L, U2R in IoT network [13]. However, Side-Channel, Man-in-the-Middle (MITM), and Malicious Code attacks have not been explored widely which occur frequently in the IoT network.

In this research, an Adaptive Neuro-Fuzzy Inference System (ANFIS) integrated SDN-IoT based Fuzzy Neural Network

(FNN) architecture has been proposed where IDS is concerned only on the perception layer, and the concept of SDN has been integrated with the IoT network for network and application layer security. The main contribution of the paper is summarized as follows:

- This research proposed an integrated SDN-IoT architecture that can detect three new attacks SC, MITM, and MC attack besides DDoS which also frequently occurred in the IoT network.
- The whole IoT network is integrated with SDN architecture where OpenFlow protocol provides the security of the network and application layer and SDN controller will analyze the traffic of the perception layer and detect attacks that ensure overall security.
- The proposed system is an ANFIS based FNN model where fuzzy logic can work on imprecise data and doesn't need a lot of data to predict the optimal result. Fuzzy makes the system a light-weight IDS as it won't affect system latency much. So these make the system optimum, efficient and user-friendly.

The rest of this work is sorted as– section II explained various types of IoT attacks, the role of SDN to detect these attack from the traffic analysis and how FNN is connected to them, The proposed attack detection model based on FNN is introduced in section III, section IV shows performance results of the proposed FNN based attack detection model, and the work has been ended with possible future research direction in section V.

II. Literature Review

This section discusses the various types of IoT attacks and the role of SDN to detect these attacks.

A. IoT Attacks

IoT adds a new paradigm in the communication and computation of raw data among an enormous number of wireless objects equipped with sensors, source nodes, Radio-Frequency Identification (RFID) devices or any embedded computing systems. Till now many variations of layered IoT architecture have been reported but the three-layered architecture, composed of perception, network and application layers, is the basic architecture of any IoT aided network. [14].

With the various extended facilities, IoT comes with a lot of vulnerabilities that result in a wide range of hazardous attacks especially in the perception layer as this layer engages with physical devices and deals with traffic flow. Hence detection and blockage of such attacks in the perception layer is of prime concern of the proposed SDN-IoT infrastructure. Object tampering, Outage attack, DDoS, Side-Channel, Camouflage, Tag Cloning, MITM, Malicious Code Injection, Social Engineering, Hardware Trojan, Tag Tampering, etc. are some of well-known attacks in the perception layer.

Among the mentioned attacks, Table I, lists the most frequently occurring attacks- MITM, DDoS, MC and SC with features as they are considered in this system [15]. The attack features assembled from various research papers, journals, websites and other resources, are the most prominent and well defined enough to characterize any of these particular attacks. According to the proposed model, the attack detection and security of network and application layer are ensured by the SDN controller.

TABLE I: Attacks Description and Features.

Attack	Features
MITM [15], [16]	• **Get SSH Alarm** for Redirecting SSH/HTTPS sessions, • Detect **twin WiFi** hotspot/doubtful service set ID, • Receive Security **certificate error message**, • Obtained **Phishing e-mail**.
DDoS [17], [18]	• Sudden **shut down** or **crash** of server, • **Server Overload** due to overflowing sensors & nodes, • Services become too **slow** even if server doesn't shut down, • Multiple **error message** from malicious nodes / any external intruder.
SC [15], [19]	• **Sudden drop of voltage** across resistor, • Excessive rate of noise **degradation in SNR** value, • **Bit flips count** in memory cells of a transistor on a micro-controller, • Unauthorized/third party **data access**, • Server **overload** & **malfunction** of targeted device.
MC [15], [20]	• Detect viruses, Trojan horses, ransomware, spyware etc, • Overload the server, • slowing down the system and overflow memory.

Legend: MITM–Man-in-the-middle attack, DDoS–Distributed denial-of-services ; SC–Side-Channel attack; MC– Malicious code attack, SNR–Signal to Noise Ratio

B. SDN

SDN introduces a promising era in networking, in which the control and data planes are decoupled and devised with three different basic layers- application, control and infrastructure layer. The control plane is software-based and can control all the connected IoT devices. SDN controller plays this role by controlling the traffic flow from a centralized user interface. Besides the functionality layers, SDN also provides two bridge layers, the Northbound and Southbound Application Programming Interface (API) to enable communication with a particular higher-level or lower-level component [21].

In SDN, network devices communicate with the SDN controller for appropriate forwarding decision or routing path information. To fulfil this purpose, Openflow is widely used and through this protocol, SDN provides the security of the network against all malicious attacks.

In this paper, a centralized SDN controller integrated FNN model is proposed to certify high network performance and better consistency.

C. FNN

FNN is the structure of Artificial Neural Network (ANN) with the replacement of fuzzy neurons instead of artificial neurons. It is the integration of neural network (NN) and fuzzy logic system (FLS), a unique framework to identify cyber-attacks efficiently. The term FNN can also be considered as Hybrid Fuzzy Neural Network (HFNN) as it's the fusion of neural networks training techniques and the interpretability of fuzzy logic [22]–[24]. An HFNN generally provides a three-layer model-

- First layer- input variables
- Second layer (hidden)- fuzzy rules
- Third layer- output variables

The first layer takes an arbitrary number of input variables, the fuzzy rule base is kept hidden in the second layer as a black box and the third layer produces the desired output. In FNN/HFNN model, fuzzification is introduced through the concept of ANFIS and any type membership function (triangular, gaussian, trapezoidal etc.) is defined to build a fuzzy logic controller [25]. While modelling FNN/HFNN two conditions must be considered- the symmetricity of fuzzy sets and the total sum of membership function have to be up to 1. The modelling of FNN/HFNN in the proposed system adds interoperability and flexibility and provides the best training and testing percentage in the detection of cyber attacks [26].

III. Proposed Attack Detection Model

This section illustrates every step for designing the proposed system model.

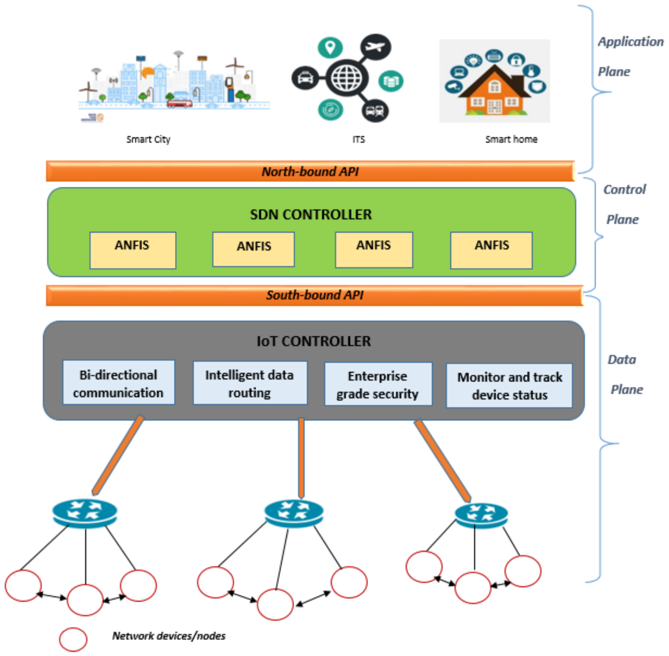

Fig. 1: Proposed system architecture. The model consists of three-layer where the data plane deals with IoT devices & network gateways through IoT controller; control plane covers FNN integrated SDN controller and application plane handles ultimate IoT applications.

A. System Architecture

The integrated SDN-IoT architecture has been proposed in Figure 1. In SDN, data and control planes work separately where the IoT controller will monitor all the data packets from nodes in a centralized way. The proposed ANFIS model inside the SDN controller monitors the traffic behaviour and detects attacks. SDN provides its own security mechanism for a network through OpenFlow protocol in the network and application layer and proposed ANFIS model secures the perception layer from cyber-attacks.

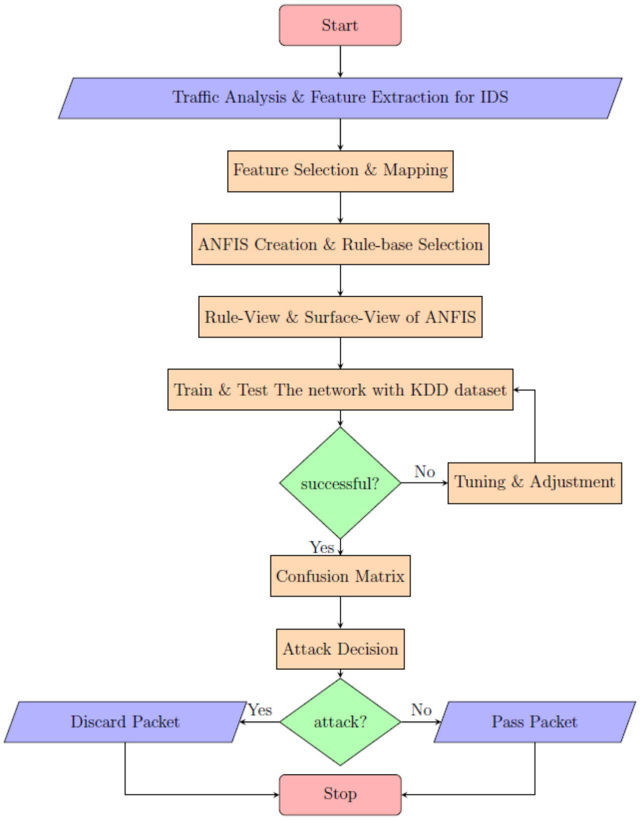
Start
Traffic Analysis & Feature Extraction for IDS
Feature Selection & Mapping
ANFIS Creation & Rule-base Selection
Rule-View & Surface-View of ANFIS
Train & Test The network with KDD dataset
successful?
No
Tuning & Adjustment
Yes
Confusion Matrix
Attack Decision
Discard Packet
Yes
attack?
No
Pass Packet
Stop

Fig. 2: Flow of IDS technique. It demonstrates modules of model formulation.

B. Methodology

1) Network Traffic Analysis (NTA): First and foremost step is to analyze network traffic which is a process of intercepting and analyzing traffic communication to detect any unusual pattern. Rule based approaches are efficiently used for internet protocol (IP) traffic classification which also prioritizes the set of features matches with the distinguished attacks [27].

2) Feature Extraction Phase (FEP): Feature extraction selects or combines variables into features after analyzing the pattern of traffic. It helps to summarize the classification of unusual behaviour which is detected by NTA. For the proposed model, initially, seventeen features have been tabulated for improved feature visualization and increase the explainability of the model. Among multiple tools, Wireshark and Net Mate are commonly used for capturing packets and feature extraction [28].

3) Feature Selection Phase (FSP): Feature selection is one of the core concepts which hugely impacts the performance of the system model. Irrelevant or partially relevant features have been excluded from the feature set to predict the most optimal output. This phase contributes a lot to improve the accuracy and decrease the training time for the model. For reducing the redundancy of the extracted feature set, the most prominent nine features have been selected to detect four frequently occurring attacks mentioned in the previous section which is the dedicated purpose of this model. WEKA is the most common tool for selecting features from the extracted feature set [28]. The selected features for the proposed model are:

- SSH Alarm,
- Server Overload,
- Error Message,
- Slow Down,
- SNR,
- Twin WiFi,
- Shut Down,
- Phishing,
- Sudden Lack of Memory Storage

4) ANFIS Designing Phase (ADP): Fuzzy logic is a form of many-valued logic which can do reasoning with all intermediate possibilities between 0 and 1. A fuzzy inference system (FIS) is a data learning technique that uses fuzzy logic to transform multiple given inputs into a desired optimum output through rules set and operations. Between two types of FIS (Mamdani, Sugeno) Takagi–Sugeno fuzzy logic is used to construct the ANFIS in the proposed model. The procedure of FIS is a combination of fuzzification module, knowledge base and defuzzification module which is done through the mapping functions derived from the input feature set [29], [30]. In this case, trapezoidal membership functions are considered.

The proposed FNN model consists of four ANFIS– ANFIS-1, ANFIS-2, ANFIS-3 and ANFIS-Decision where the output of the first three ANFIS work as the input for ANFIS-Decision. So the system mostly depends on the last one.

According to the system design, attack features of the four aforementioned attacks are the inputs of different ANFIS. ANFIS-1 takes four inputs- SO (Server Overload), SD (Slow Down), ShDn (Sudden Shut Down) and EM (Error Message). As these inputs are related to all attacks, the output demonstrates the four attacks' initial probability. The attacks are ranked according to the maximum match with input features. So the output mapping function value of ANFIS-1 is considered as- DDoS (90), MITM (15), SC (40), and MC (65). As a result, ANFIS-1 predicts DDoS when output goes high, MITM attack at low and others according to the range.

Figure 3 shows the input membership functions for the ANFIS-1 after training and Figure 4 is the ANFIS-1 surface view. Due to the page limitation, we have not shown the input and output for ANFIS-2 and ANFIS-3.

In ANFIS-2, inputs are PH(Phishing), TW(Twin Wifi) and SA(SSH Alarm) which matches most with the features of MITM so it can easily detect MITM.

ANFIS-3 takes two inputs: SNR and MEM (sudden lack of memory) that match the feature of SC and MC. Output depicts SC Attack when it's low and MC Attack when it's high.

As the above three outputs work like inputs of ANFIS-Decision(see Figure 6), it means it can combine the features of different ANFIS to detect the attack significantly. For instance, if ANFIS-1 gives a low value which means MITM and ANFIS-2 provide high value that results in MITM, then it combines the features of two ANFIS and decides MITM certainly.

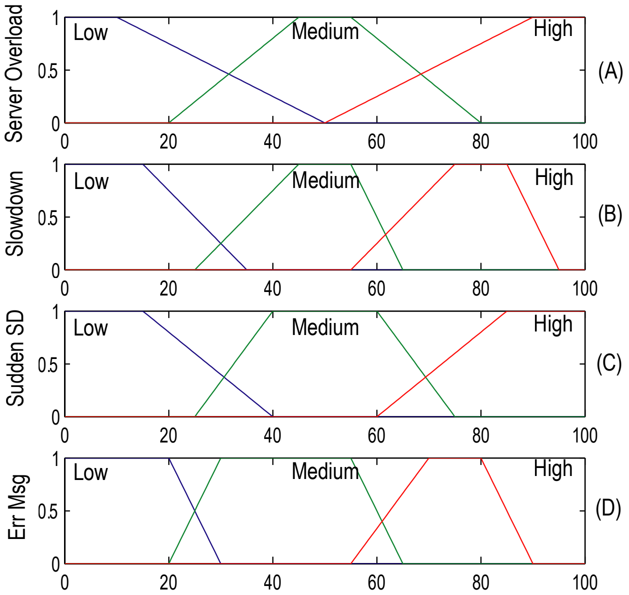

Fig. 3: Input membership variables for ANFIS-1 (A) shows linguistic values of Server Overload (B) shows linguistic value of Slowdown (C) shows linguistic values of Sudden ShutDown and (D) shows linguistic values of Error Message.

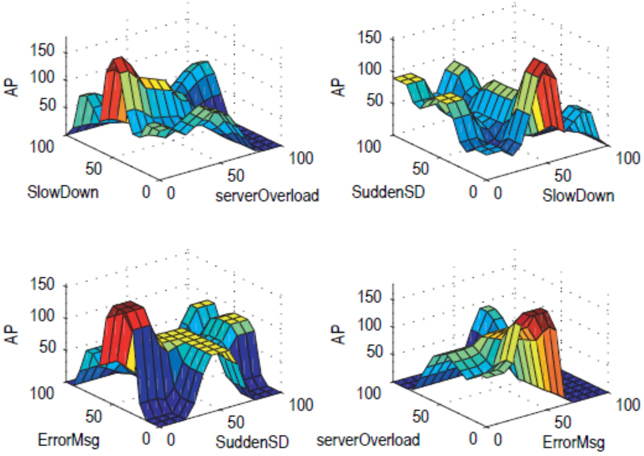

Fig. 4: Surface view of ANFIS-1 that depicts input and output relation in the rule base of it.

Figures 5 (A)–(C) show the surface view which depicts input and output relation in the rule base of Decision FIS.

In Figure 5(D), the mapping function has been designed in ranges from 0 to 1. The range value of each attack is defined based on "common characteristics" logic. As DDoS and MC

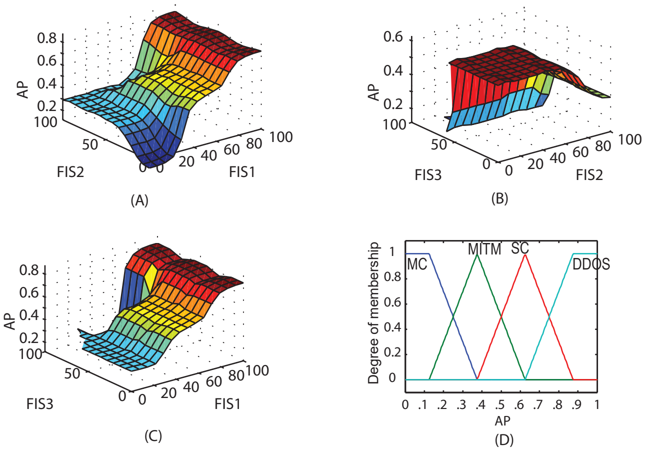

Fig. 5: (A)-(C) Surface view of input and output relation in the rule base of Decision FIS. (D) Output membership variables.

attacks have most matched features so they have been kept far away to avoid the feature collision. On the contrary MC and MITM has only one common feature which creates no problem to fix them with the nearest range value. The ranges are considered as MC $\in [0.0 - 0.25]$; MITM$\in [0.25 - 0.5]$, SC $\in [0.5 - 0.75]$, and DDoS $\in [0.75 - 1]$

IV. Performance Analysis

This section includes the performance evaluation of the proposed FNN based attack detection system. The FNN model is simulated in the Matlab-Simulink and the model is trained and tested using the NSL-KDD attack dataset [12], [31] which is the modified version of KDD'99 data set. Our simulation set up consists of four ANFIS blocks (named ANFIS-1, ANFIS-2, ANFIS-3 and ANFIS-Decision).

The prototype of the system network model in Matlab-Simulink shows the success of the detection attack pictorially. For instance, in Figure 6, at first EM value is 90 which is high, makes ANFIS-1 output as MITM; secondly, in ANFIS-2, PS and SA values are high (80 & 75) and TW is medium (45) which overall makes the ANFIS-2 output high; and finally, ANFIS-3 input SNR is 85 that is high and MEM is 15 that is low, which ends up with No Attack in ANFIS-3. So this instance should demonstrate the attack probability of MITM, ranged in 0.25 to 0.5 and here the test result exhibits 0.38 that establishes the MITM attack as it is in the above range.

In this SDN-IoT integrated system, SDN controller acts as an adaptive firewall after malicious traffic detection. It removes malicious packets, blocks suspicious hosts and further observes for questionable activities in the network.

For training and testing of the system, KDD-NSL Dataset is used in this research [10]. Though KDD Dataset specifies DDoS, Probe, U2R, R2L attack [31]; the designed FNN system is compatible with some features of KDD-NSL dataset. The mapping among KDD feature set and input of ANFIS-Decision is depicted in Table II:

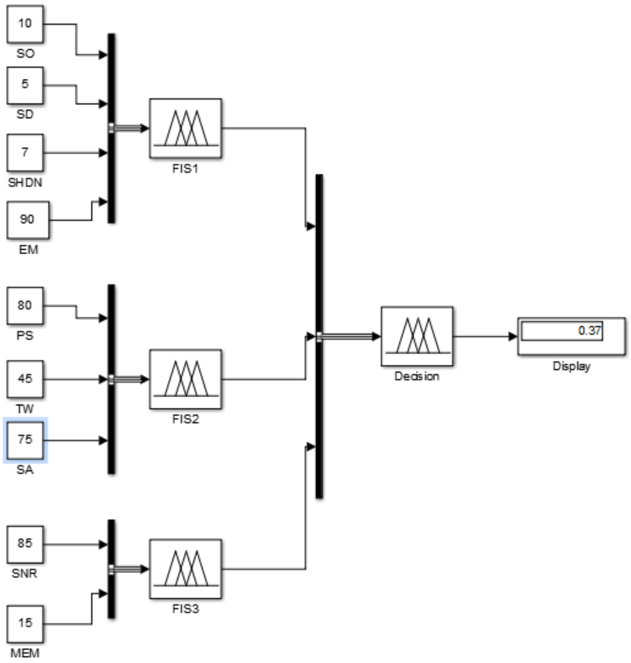

Fig. 6: Simulink model for attack detection. The model contains four ANFIS blocks: ANFIS-1, ANFIS-2, and ANFIS-3 take input features (See Table II) from the traffic flow data analyzed by SDN. Finally, ANFIS-Decision detects one of the four attacks such as MITM, DDoS, SC, and MC.

TABLE II: KDD Feature [10] in relation with our proposed model.

Input	KDD Dataset Feature
FIS-1	Service, Hot, Flag, Num_failed_logins, Serror_rate, Srv_serror_rate, Root_shell, Num_root, Num_file_creations, Num_shells, Num_access_files, Srv_count, Same_srv_rate, Diff_srv_rate, Srv_diff_host_rate, Dst_host_count, Dst_host_srv_count, Count, Dst_host_same_srv_rate, Dst_host_diff_srv_rate, Dst_host_same_src_port_rate, Dst_host_serror_rate, Dst_host_srv_serror_rate
FIS-2	Src_bytes, Dst_bytes
FIS-3	Duration, Src_bytes, Dst_bytes, Urgent, Hot, Srv_count, Serror_rate, Srv_serror_rate ,Same_srv_rate, Diff_srv_rate, Srv_diff_host_rate, Dst_host_count, Dst_host_same_srv_rate, Count, Dst_host_diff_srv_rate, Dst_host_diff_srv_rate, Dst_host_same_src_port_rate, Dst_host_srv_diff_host_rate, Dst_host_serror_rate

Legend: Num–Number; Srv–Server; Diff–Different; Dst–Destination; Src–Source; Serror–Synchronization Error

In a confusion matrix, performance measurement is done by comparing the actual class labels and the predicted class labels for each of the individual classifiers of the system model. A 4×4 confusion matrix is generated here after training and testing of the system model which is drawn in figure 7:

From the confusion matrix, the values of accuracy, precision, recall and F1-score for four mentioned attacks detection are generated and presented in the figure 8:

The evaluation of performance exhibits that the proposed FNN system can detect four above-mentioned attacks with an overall accuracy of 83%.

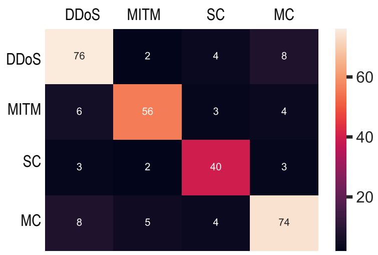

Fig. 7: Confusion Matrix for DDoS, MITM, SC, and MC. The figure reveals that the proposed system can detect the four mentioned attacks with high accuracy.

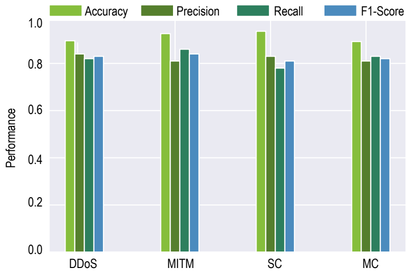

Fig. 8: The performance of proposed attack detection model using FNN and SDN. The figure shows that the proposed system detects the DDoS attack with the highest accuracy.

V. Conclusion

This work has proposed the attack detection model for IoT using a Software-defined network (SDN). The SDN controller can analyze the traffic flow, detect the anomaly, and block incoming traffic as well as the source nodes. In the SDN, an FNN based attack detection system is considered which can detect attacks such as man-in-the-middle, distributed denial-of-services, side-channel, and malicious code. The simulation model is implemented in the Matlab-Simulink, the fuzzy rule-based system is designed using expert opinion and the model is trained and tested using the extracted attack features from the NSL-KDD data sets. The confusion matrix analysis reveals that the proposed FNN based attack detection system can detect the mentioned four attacks with high accuracy. Finally, accuracy, precision, recall, and F-1 score show the model can detect various attacks in the IoT system. In the future, we are interested in employing deep machine learning based feature extraction and classification technique to detect the various attacks in IoT in real-time.

References

[1] M. Asif-Ur-Rahman and et al., “Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4049–4062, 2019.

[2] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, “Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN),” *Computers*, vol. 9, no. 1, p. 8, Mar. 2020.

[3] M. Mahmud *et al.*, “A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications,” *Cogn. Comput.*, vol. 10, no. 5, pp. 864–873, Oct. 2018.

[4] M. Nobakht, V. Sivaraman, and R. Boreli, “A host-based intrusion detection and mitigation framework for smart home iot using openflow,” in *2016 ARES*. IEEE, 2016, pp. 147–156.

[5] N. Abdolmaleki, M. Ahmadi, H. T. Malazi, and S. Milardo, “Fuzzy topology discovery protocol for SDN-based wireless sensor networks,” *Simul. Model. Pract. Theory*, vol. 79, pp. 54 – 68, 2017.

[6] M. D. Alshehri and F. K. Hussain, “A fuzzy security protocol for trust management in the internet of things (fuzzy-iot),” *Computing*, vol. 101, no. 7, pp. 791–818, 2019.

[7] M. Ge and et al., “Deep learning-based intrusion detection for iot networks,” in *2019 IEEE PRDC*. IEEE, 2019, pp. 256–25 609.

[8] Y. Zhang, P. Li, and X. Wang, “Intrusion detection for iot based on improved genetic algorithm and deep belief network,” *IEEE Access*, vol. 7, pp. 31 711–31 722, 2019.

[9] Y. Miah and et al., “Performance comparison of machine learning techniques in identifying dementia from open access clinical datasets,” in *Proc. ICACIn*. Springer, Singapore, 2020, pp. 69–78.

[10] University of New Brunswick, “Datasets | Research | Canadian Institute for Cybersecurity | UNB,” 2015, library Catalog: www.unb.ca. [Online]. Available: https://www.unb.ca/cic/datasets/index.html

[11] W. Li, S. Tug, W. Meng, and Y. Wang, “Designing collaborative blockchained signature-based intrusion detection in iot environments,” *Future Gener. Comput. Syst.*, vol. 96, pp. 481 – 489, 2019.

[12] P. S. Bhattacharjee, A. K. Md Fujail, and S. A. Begum, “A comparison of intrusion detection by k-means and fuzzy c-means clustering algorithm over the nsl-kdd dataset,” in *2017 IEEE ICCIC*, 2017, pp. 1–6.

[13] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the kdd cup 99 dataset,” in *SSCI*. IEEE, 2009, pp. 1–6.

[14] M. Nawir *et al.*, “Internet of things (iot): Taxonomy of security attacks,” in *2016 ICED*. IEEE, 2016, pp. 321–326.

[15] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, “A comprehensive iot attacks survey based on a building-blocked reference model,” *Int. J. Adv. Comput. Sci. Appl.*, pp. 355–373, 2018.

[16] L. Wang and A. M. Wyglinski, “Detection of man-in-the-middle attacks using physical layer wireless security techniques,” *Wireless Communications and Mobile Computing*, vol. 16, no. 4, pp. 408–426, 2016.

[17] K. Sonar and H. Upadhyay, “A survey: Ddos attack on internet of things,” *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.

[18] J. Kaur and A. B. Gandhi, “Security and ddos mechanisms in internet of things,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 9, 2017.

[19] J. He, Q. Xiao, and M. S. Pathan, “A method for countering snooping-based side channel attacks in smart home applications,” in *EAI Chinacom*. Springer, 2016, pp. 200–207.

[20] D. Wei and X. Qiu, “Status-based detection of malicious code in internet of things (iot) devices,” in *2018 IEEE CNS*. IEEE, 2018, pp. 1–7.

[21] K. S. Sahoo, B. Sahoo, and A. Panda, “A secured sdn framework for iot,” in *2015 MAMI*. IEEE, 2015, pp. 1–4.

[22] D. Souza and et al., “Detection of anomalies in large-scale cyberattacks using fuzzy neural networks,” *AI*, vol. 1, no. 1, pp. 92–116, 2020.

[23] M. S. Kaiser *et al.*, “Fuzzy logic based relay search algorithm for cooperative systems,” in *2009 ICSNW*, 2009, pp. 1–7.

[24] ——, “Advances in crowd analysis for urban applications through urban event detection,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 10, pp. 3092–3112, 2018.

[25] “Fuzzy neural network - scholarpedia,” http://www.scholarpedia.org/article/Fuzzy_neural_network, (Accessed on 05/09/2020).

[26] L. O. Batista *et al.*, “Fuzzy neural networks to create an expert system for detecting attacks by sql injection,” *arXiv preprint :1901.02868*, 2019.

[27] T. T. Nguyen and G. Armitage, “A survey of techniques for internet traffic classification using machine learning,” *IEEE Commun. Surv. Tutor.*, vol. 10, no. 4, pp. 56–76, 2008.

[28] H. K. Gill and M. Singh, “Analyze university network traffic to explore usage behaviour and to detect malicious activities,” in *2015 NGCT*, 2015, pp. 686–691.

[29] S. Rahman *et al.*, “Phy/mac layer attack detection system using neuro-fuzzy algorithm for iot network,” in *IEEE ICEEOT*, 2016, pp. 2531–2536.

[30] M. S. Kaiser *et al.*, “A Neuro-Fuzzy Control System Based on Feature Extraction of Surface Electromyogram Signal for Solar-Powered Wheelchair,” *Cogn. Comput.*, vol. 8, no. 5, pp. 946–954, Oct. 2016.

[31] P. Aggarwal and S. K. Sharma, “Analysis of kdd dataset attributes-class wise for intrusion detection,” *Procedia CS*, vol. 57, pp. 842–851, 2015.