Internet of Things 3–4 (2018) 82–89

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Deep learning and software-defined networks: Towards secure IoT architecture

Ahmed Dawoud*, Seyed Shahristani, Chun Raun

School of Computing, Engineering, and Mathematics, Western Sydney University, Sydney, Australia

ARTICLE INFO

Article history:
Received 29 August 2018
Accepted 1 September 2018
Available online 6 September 2018

Keywords:
Internet of Things
Software-defined networks
Anomalies detection
Deep learning
Restricted-Boltzmann machines

ABSTRACT

Internet of Things (IoT) introduces new challenges to conventional communication model. IoT networks characteristics, such as objects heterogeneity and scalability, require revolutionary solutions. Currently, there is no universal architecture for IoT. However, several architectures were proposed based on Software Defined Networks (SDN). SDN introduces network programmability, and centralisation, these features facilitate network abstractions, simplifying network management and eases evolution. In this paper, we investigate SDN as a novel communication architecture for IoT networking to enhance the security and resilience of IoT. SDN enhances network resilience and scalability which are essential in large-scale IoT deployments, e.g., smart cities. However, security is a significant concern for IoT while SDN deepens these concerns. SDN itself presents new security threats; specifically, threats related to the controller.

We propose a secure, framework for IoT based on SDN. The framework is generalization for the integration of SDN and IoT. We focus on massive IoT deployment, for instance, smart cities applications, where, security is critical, and network traffic is enormous. The study investigates the SDN architecture from a security perspective. Improving SDN security will boost the deployment of SDN-based IoT architecture.

We deploy an Intrusion detection system based on Deep Learning (DL). The detection module uses Restricted Boltzmann Machines (RBM). The precision rate shows significant improvements over standard ML, e.g. SVM and PCA.

1. Introduction

Internet of Things expands the presence of the internet by connecting smart objects, for instance, grid, health, and environmental devices. The advancement in wireless communication, embedded systems, and sensors technologies accelerate the adoption of IoT model in several domains. However, the higher connectivity is kind of equivalent to increasing privacy and security threats.

IoT introduces three challenges. The first challenge is the heterogeneous composition of the network. Secondly, IoT adopts hugely distributed architecture, specifically in applications like smart cities and smart grids. Thirdly. IoT introduces new protocols to handle specific issues related to power and computation limitation of the network sensors [1].

The IoT threats vector extended with new attacks, for example, by cloning the object, firmware replacement, security parameters extraction [1,2].

* Corresponding author.
E-mail address: a.dawoud@westernsydney.edu.au (A. Dawoud).

https://doi.org/10.1016/j.iot.2018.09.003
2542-6605/

Software-Defined Networks (SDN) networking model detaches control and forward planes [3]. The devices provide forwarding capabilities to switch the data flow, while the control plane is decoupled to introduce a new entity called the network controller. The forward plane located at the bottom of the stack includes hardware devices, e.g., switches, routers, and firewalls and Intrusion Detection Systems (IDS). The devices do not possess the software intelligence needed to fill the forwarding tables. The network logic independently relocated to the controller layer.

The controller abstracts the devices and provides resources required to programme low-level forwarding devices. Controller aka Network Operating system (NOS) provides services like network state, and topology information. Additionally, the controller provides northbound, and southbound APIs. The northbound API to facilitate communication with the applications. Whereas, the southbound API to provide accessibility between the controller and forwarding devices. OpenFlow is a defacto SDN southbound protocol [4].

SDN is a novel networking paradigm that improves flexibility, scalability, and security [3]. There are several research papers on deploying an SDN as the networking model for IoT [2,5–14]. However, security is a major concern in SDN [2].

Machine learning had been used for network anomalies detection; however, the precision of detection was not practically efficient.

The recent advances in DL started in 2006 by a pre-training step using restricted Boltzmann Machines (RBM) [15]. Later, various algorithms were proposed to solve problems in neural networks, e.g., the generalization problem.

This work focuses on enhancing the security of IoT architecture based on SDN. We adopt an intrusion detection approach to protect the network. The current success of applying deep learning in several applications is promising and motivates the application of DL methods in network anomalies detection. In section two we present related work this includes various deployment of SDN and IoT and application of DL for anomalies detection. In section three we discuss the security issues of SDN specifically, threats related to the controller. In section five we propose a generic architecture for IoT based on SDN, and we present the detection system. Subsequently, we introduce an experimental evaluation of the detection system.

2. Related work

Several studies proposed SDN based architecture to enhance the security of IoT; Studies [5,7] considered a domain-based architecture, where the network includes multiple domains. The separation of domains enhances the availability of the network. However, there is no robust performance analysis.

Bhunia and Gurusamy proposed a detection system based on SDN for DoS of IoT [9]. The authors claimed they achieved a precision of around 98%. Chakrabarty et al. proposed a SDN based IoT architecture called Black SDN [10]. Black SDN secures payload and Metadata through encryption. However, the routing suffers complications as the source, and destination data in the header are encrypted too. Jararweh et al. focused on IoT management aspects by proposing a comprehensive SDN based architecture to enhance the IoT management SDIoT [11]. The framework enhances the forwarding, storing, and securing data generated from the IoT objects.

With a specific focus on Denial of Services attacks DoS, Bull et al. presented a flow-based detection system implemented in SDN gateway to detect and mitigate DoS [12]. However, the study lacked proven performance and efficiency analysis.

A study utilizes deep learning for anomalies detection in IoT networks. They used unsupervised deep learning algorithm. However, the study lacked details about the detection framework, for instance, how to decide upon anomalies? Is a threshold used?

Hodo et al. deployed a multi-layer Artificial Neural Network (ANN) for IoT anomalies detection. The authors' results showed 99.4% of accuracy, and the capability to detect any DoS attacks [14].

Fiore et al. used semi-supervised deep learning for network anomalies detection [16]. Authors introduced a discriminative form of restricted Boltzmann machines. The results were not promising, specifically, when testing the DRBM in a new network.

Several research papers focus on improving the classical machine learning algorithms with deep learning. Salama et al. used Deep Belief Network (DBN) as a dimensionality reduction tool for Support Vector Machines (SVM) classifier [17]. The authors claimed a hybrid approach achieve approximately 93% accuracy where the SVM and DBN scored 88% and 90%, respectively. In another comparative study, authors compare three traditional algorithms, i.e., Bays networks, C4 and SVM against a hybrid SVM-RBM algorithm. The results showed the superiority of the hybrid method in various attack detection, e.g., DoS and user root attacks [18]. In a broader comparative study on anomalies detection, authors presented a deep structured energy-based model; The study compares their algorithms in two different decisions boundaries against five severe anomalies detection algorithms including PCA and SVM. The authors go further step by applying their algorithm to various data types, i.e., static, sequential, and spatial datasets [19]. Among the static datasets, they choose the KDD99 network dataset. Their results showed comparable or better performance to methods like PCA and kernel PCA.

This work introduces the integration of SDN and DL in a single framework to enhance the security of IoTs for IoT. SDN has been introduced to IoT to tackle challenges related to the rigorous architecture of conventional communications networks, for instance, resilience and scalability. However, SDN suffers serious security deficiencies; we analyzed this threat experimentally in details. SDN itself need security measures [20]. In this study, we propose a centralized detection system based on DL to enhance the security of SDN, subsequently, improves the security of IoT.

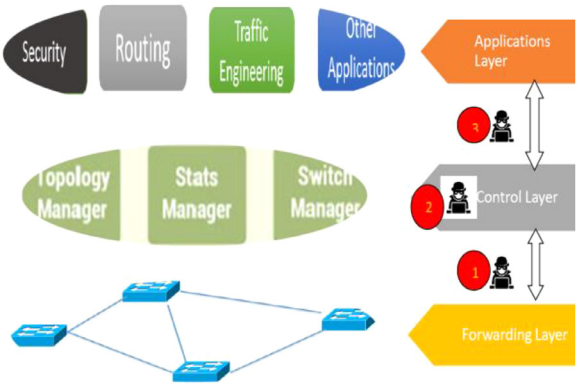

Fig. 1. Controller security threats.

3. Security issues in SDN

Network programmability is a key privilege achieved by SDN model, where applications in the top plane can access the physical devices through the controller. Programmability facilitates and accelerates the innovation with an enormous number of network applications, e.g., monitoring, traffic engineering, security, and cloud applications. Centralization is an essential characteristic of the SDN architecture. A controller is a central entity which provides a global view of the entire network; it eases the management and policies enforcement process. Additionally, it decreases the faults in configuring and deploying the network policies. The centralization enhances the network resilience and interoperability, for instance, multiple of devices from various industrials can be integrated and abstracted in one network.

Security threats are critical challenges in conventional networking systems. The threats are intensifying in SDN networks. The model's many advantages are accompanied by additional threats that were not possible in the traditional networks. For the southbound OpenFlow protocol, a security analysis study exposed various attacks derived from the SDN standard protocol, for example, flow tables and on the devices control channels between the devices and controller affected by a denial of service attacks (DoS). Application privilege conflicts propagate to flow rules. The control channel between the controller and the switch is initiated as a TCP connection, with an option for encryption protocol Transport Layer Security (TLS) to secure the channel. Without an encryption method, the communication between the controller and the forwarding devices are exposed to a man in the middle attacks. Kloti et al. have conducted a security analysis for the OF protocol [21]. The study has deduced that denials of services attacks have threatened the flow tables and the communication channels; as the attacker flood those components with OpenFlow rules and requests. Additionally, tampering attacks have substantially targeted the flow tables on the devices by installing rules from untrusted sources.

Kreutz et al. concluded seven threats vector for SDN [2]. Three threats are directly linked to the controller itself as shown in Fig. 1,

1. Attacks on the communications between the controller and the data plane devices.
2. Attacks on the controller vulnerabilities.
3. Attacks on the controller originated from untrusted applications.

Intrusion Detection Systems are software or hardware systems dedicated to monitoring the traffic for security threats. Standard intrusion detection process includes three phases, collecting data from the network, analyzing, and then launch a proper response if a threat exposed. There are three approaches to analyze the collected traffic named signature-based, anomaly detection, and specification based. Firstly, signature-based, whereas a system has a database of predefined violations' signatures, and the system matches those signatures against the network activity signatures. Secondly, anomalies or outlier analysis, the system concerns about differentiate between the normal and abnormal patterns. For the system, normal activities are identified in a baseline profile, which the system develops in a learning phase. Thirdly the stateful protocol analysis, in this method a predefined pattern of protocols' behaviour is established, a comparison is made between network activities and the expected behaviour defined by protocols, and in the case of profile violation, an alert is raised. A combination of Methods is used to maximise the IDP performance. A significant weakness in the signature-based method is the inability to detect new attacks while the anomaly detection has a higher false alarms rate. The majority of the commercial implementations use a hybrid approach [22,23].

Anomalies or outliers are unexpected patterns. In the context of networking, we assume the intrusion or attacks are unusual behaviour]. So at any point, the majority of the traffic is normal. Several approaches were adopted .e.g. statistical methods, machine learning, and biological models. The proposed framework adopts a machine learning approach.

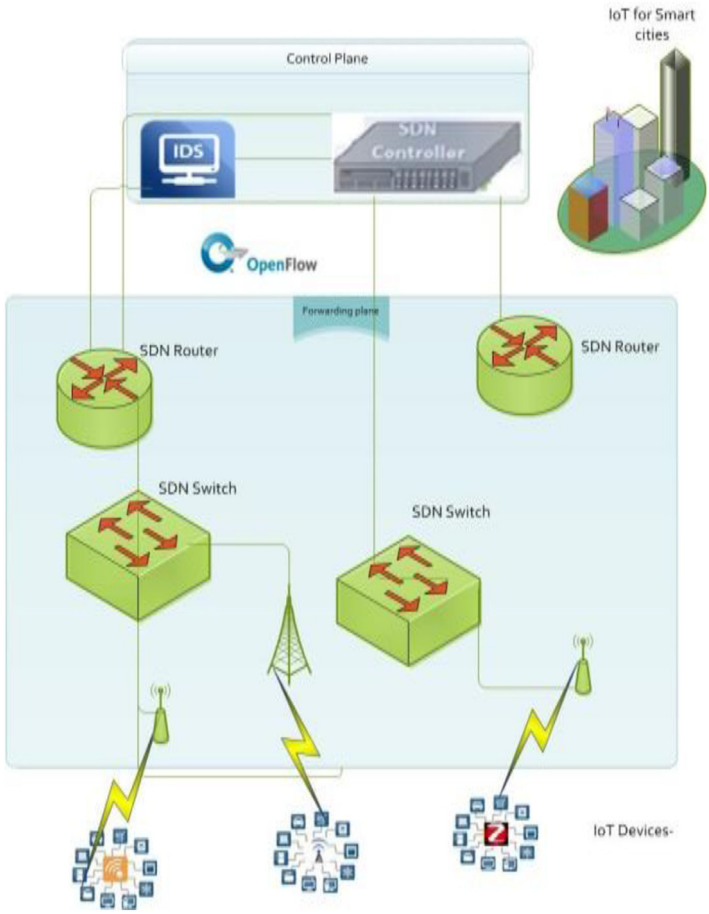

Fig. 2. Proposed SDN-based IoT architecture with Detection framework.

4. Proposed architecture, detection system

In this section, we propose a secure, resilient and scalable architecture for IoT. We focus on massive IoT deployment, for instance, smart cities applications, where, security is critical, and network traffic is enormous. The study investigates the SDN architecture from a security perspective. We deploy an intrusion detection system based on deep learning. Improving SDN security will boost the deployment of SDN-based IoT architecture. The proposed detection system utilizes deep learning for network anomalies detection.

Fig. 2 depicts SDN-based IoT architecture. The bottom layer includes IoT devices, e.g., sensors. SDN layers top the IoT devices, i.e., forward and control layers. We proposed a detection system at the controller layer. This deployment allows the IDS system to interact directly through the network hence protect the controller itself. The deployment of IDS at the application layer will not avoid the controller threats.

RBMs are energy based models, where each feature configuration is assigned scalar energy. The learning process will modify the energy function so the shape will have desirable properties. The probability distribution of energy function as in formula (1.1)

$$p(x) = \frac{e^{-E(x)}}{Z}, \tag{1.1}$$

where Z is the partitioning function defined as (1.2)

$$\mathrm{Z} = \sum_{x} e^{-E(x)} \tag{1.2}$$

Boltzmann machines energy function is (1.3)

$$E\ (x) = -\ x^T\ W\ x - b^T x, \tag{1.3}$$

where W is weight matrix and b is bias parameter

To enhance the RBM, the hidden units are introduced. RBMs are forms of BMs with restrictions on connections between visible- visible and hidden-hidden units. The energy function of RBMs is represented in (1.4)

$$E\ (v, h) = \ -b'v - c'h - h'Wv \tag{1.4}$$

where b' and c' are the bias for visible and hidden units respectively and W are the weights of the connections between hidden and visible units. compute the data loss, for instance, the squared error function. The third step is to minimize the cost (in our case data loss). Several optimization algorithms are used to minimize the loss or reconstruction rate. For example, we used Adam optimizer. Once the network settles after various sweeps of data chunks (batches), the second phase testing during the testing, we feed the network with the testing samples and try to reconstruct the data.

For the anomalies detection, we measure the data loss between the input and the reconstructed record. If the loss is too high (we have to define thresholds) this means the input cannot be precise enough to be reconstructed. We consider inputs with high reconstruction error as anomalies. This concept is valid for Restricted Boltzmann machines, as both algorithms reconstruct the input.

The performance of the algorithm varies depending on various criteria.

- Type of the data, whether the input is binary or decimal.
- Activation function, for example, sigmoid works better with binaries while Relu is good for decimals.
- The cost function, for instance, squared error, and cross entropy.
- Optimizer, Gradient Descent, Adam optimise, SGD (figure below shows cost optimisation using two different optimisers). The autoencoder aims to minimize the reconstruction error over multiple sweeps of the input data. The y-axis represents the data loss calculated by the cost function (squared error), while the x-axis represents the data sweeps. The graph shows the loss is decreased until it reaches the minima.

Algorithm anomalies detection:

Data: network traffic records (continuous and digit values) D
Input: t $\in$ $T_0..T_k$ where T is 1* 42 tensors and k = no of traffic records in the normalised dataset DNT generated by scaling k samples of the D
Output: A Set of clusters $C_0...C_n$ each, where each C is Normal or abnormal
Procedure
Training:
Let EP no of epochs
Let s = batch size and no of batches BN = DN/s;
Let i,z = 0;
While (i < EP) do:
For (z = 0; z < BN; z++):
    For each t:
        Pass t through the RBM network
        Calculate weights and biases after reconstruction
Update RBM Weights W, Biases b
EP++
Return RBM trained model with updated weights and biases
Testing:
For each ts $\in$ Ts, where ts $\notin$ T
    Pass ts through the RBM
    Calc Reconstruction Error RE tensor
Pass ts to K-means
Return $C_0...C_n$ of RE

5. Simulation

In our experiment, we focus on the evaluation of the detection system. We used Tensorflow as a deep learning development library. Tensorflow is matrices flow in a graph model. TF graph consists of nodes and edges; nodes represent mathematical operations, edges represent multi-dimensional data arrays (tensors). The network model was implemented, by defining tensors for the input, weights, biases, and the output. The RBM network composed of two layers visible and hidden. The visible layers consist of 41 nodes (the number of the feature in the data et). The hidden layers neurons will be inactivated or deactivated based on the activation function of the input neurons. Also, we defined weights between the visible and the hidden layers; the weight tenors is no visible layers neurons some hidden layers neurons, where each element of the tensor represent the weight between two of the visible and hidden neurons.

The RBM network works in two-phased the forward and backward. In the forward pass, the hidden nodes will be turned on/off depending on input, weights, biases and activation function, the decision at the beginning is stochastic. The output of this pass will be a probability vector for each of the output nodes the dimensions of this tensor equal to (1* hidden nodes). Then we do sampling on the whole output tensor. In the backward phase, the sample selected for the output will be the input, and the output from this phase is a reconstructed input. We measure the loss between the input and the reconstructed input then we optimize the weights to minimize the loss.

KDD99 is the most used dataset in machine learning and intrusion detection. The dataset represents real network traffic collected data. The dataset includes 4,898,431 traffic records for the training, 311,029 records for testing. The dataset

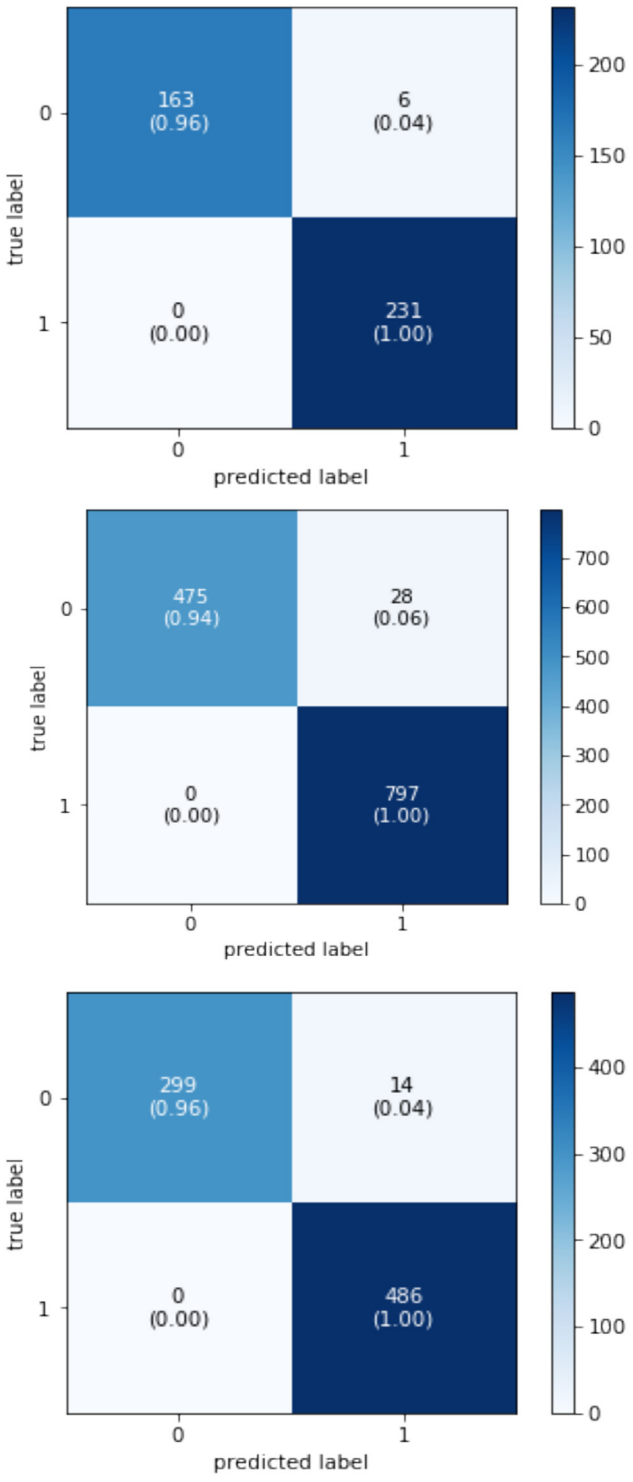

Fig. 3. Confusion matrix for samples of different sizes.

contains four types of attacks, i.e., denial of service attacks represent the most extensive traffic record, probe attacks or reconnaissance attacks, remote to local attack, and user to root attack [24]. There are several critics for KD99, for example, it is artificially generated by injecting the attacks into.

Various data-sets were built by revising KD99. However, KD99 still the most dominant we for network anomalies detection. We preferred it as we benchmark our results against another approach.

Fig. 3 shows the confusion matrix derivation for three different samples passed through the proposed system.

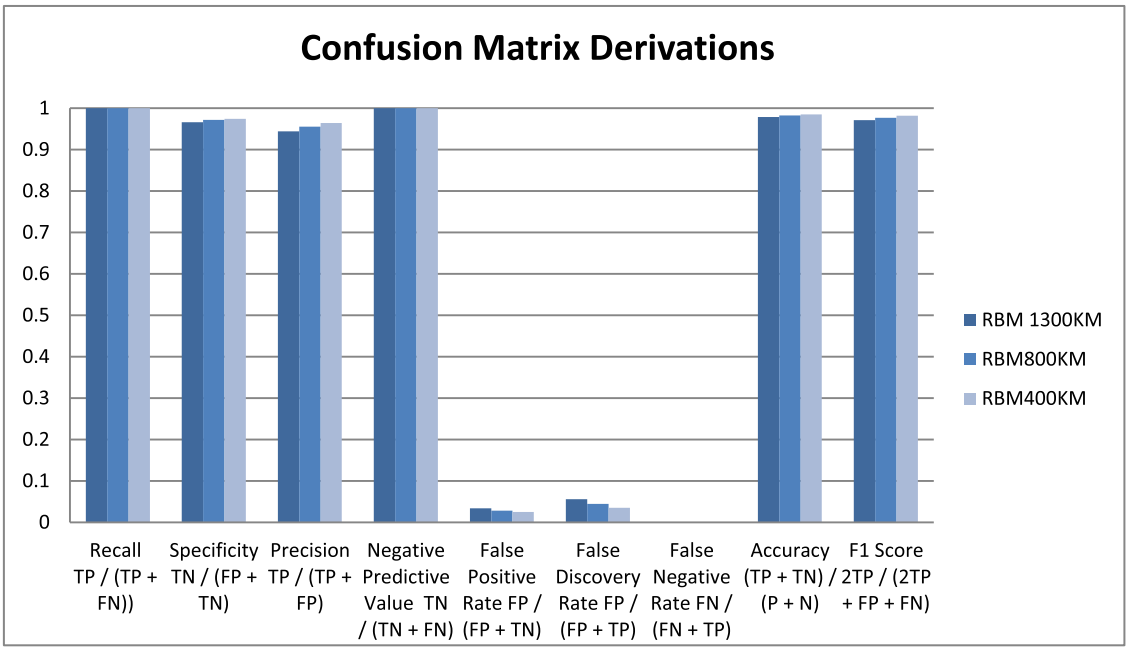

Fig. 4. Confusion Matrix complete statistics.

Table 1
Precision for different method .

Method	Precision
PCA	0.8312
Kernel PCA	0.8627
KDE	0.8119
RKDE	0.8596
OC-SVM	0.8050
AEOD	0.7624
DSEBM–r	0.8521
DSEBM–e	0.8619

The samples contain random network traffic consist of normal and abnormal traffic. The samples are labelled in the dataset; we refer to the label for results verification. There are four variables to represent various derivations.

- True positives (TP): These are samples predicted normal and they normal.
- True negatives (TN): We predicted abnormal, and they abnormal.
- False positives (FP): We predicted abnormal, but they normal. (Also
- False Negatives (FN): We predicted normal, but they abnormal.

Fig. 4 shows the confusion matrix for our two classes normal or abnormal. The top left and bottom right squares represent the precision = TP/(TP + FP), and recall = TP/(TP + FN) the top right and bottom left squares represents False Discovery Rate FP / (FP + TP) and False Negative Rate FN / (FN + TP).

In [17] Authors used RBM-SVM, SVM, and Naïve Bayes on KDD99 they claimed their best precision 85% by RBM-SVM. A recent study deployed DRBM; the results show the accuracy of 85% [15]. In the more comprehensive study, the paper compares the energy model against several ML algorithms; the precision was around 85% shown in Table 1. Our approach achieved precision higher than 94% and slightly higher accuracy.

6. Conclusion

SDN model introduces significant improvements to current networking paradigm. IoT is one domain where SDN can prevail. SDN was proposed to enhance the resilience, scalability, and security of the IoT. Deploying IoT on SDN-based infrastructure can improve IoT security, by implementing various security applications at application plane. However, SDN has major security vulnerabilities, specifically, the threats related to the network controller.

The paper introduces a detection system based on current advances in machine learning, to enhance the security of SDN based architecture of IoT. Our approach utilises the Restricted Boltzmann Machine to detect anomalies. The simulation results show a significant precision rate of over 94%.

In the study, we focused on the implementation and evaluation of our proposed detection system. In this study, we proposed a general framework for integration between IoT and SDN. However, our architecture represents general integration of IoT and SDN the. Further analysis is required practical implementation of the proposed architecture.

References

[1] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: Perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.
[2] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28.
[3] D. Kreutz, F.M.V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, S. Uhlig, Software-defined networking: a comprehensive survey, Proc. IEEE 103 (1) (2015) 14 76.
[4] N. McKeown, et al., OpenFlow: enabling innovation in campus networks, SIGCOMM Comput. Commun. Rev. 38 (2) (2008) 69–74.
[5] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of Things security: a top-down survey, Comput. Netw. 141 (2018) 199–221.
[6] O. Flauzac, et al., SDN based architecture for IoT and improvement of the security, in: Proceedings of the IEEE Twenty-Ninth International Conference Advanced Information Networking and Applications Workshops (WAINA), South Korea, 2015, pp. 688–693.
[7] C. Gonzalez, et al., A novel distributed SDN-secured architecture for the IoT, in: Proceedings of the IEEE International Conference Distributed Computing in Sensor Systems (DCOSS), Washington, USA, 2016, pp. 244–249.
[8] C. Gonzalez, et al., SDN-Based Security Framework for the IoT in Distributed Grid, in: Proceedings of the IEEE International Multidisciplinary Conference Computer and Energy Science (SpliTech), Croatia, 2016, pp. 1–5.
[9] S.S. Bhunia, M. Gurusamy, Dynamic attack detection and mitigation in IoT using SDN, in: Proceedings of the Twenty-Seventh International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, 2017, pp. 1–6.
[10] S. Chakrabarty, D.W. Engels, A secure IoT architecture for Smart Cities, in: In 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 812–813.
[11] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, A. Rindos, SDIoT: a software defined based Internet of Things framework, J. Ambient Intell. Humaniz. Comput. 6 (4) (2015) 453–461.
[12] P. Bull, et al., Flow based security for IoT devices using an SDN gateway, in: Proceedings of the IEEE Fourth International Conference Future Internet of Things and Cloud (FiCloud), Austria, 2016, pp. 157–163.
[13] K. Kalkan, S. Zeadally, Securing Internet of Things (IoT) with Software Defined Networking (SDN), in: IEEE Communications Magazine, 2017, doi:10.1109/MCOM.2017.1700714.
[14] E. Hodo, et al., Threat analysis of IoT networks using artificial neural network intrusion detection system, in: Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, 2016, pp. 1–6.
[15] A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Gener. Comput. Syst. 82 (2018) 761–768.
[16] G.E. Hinton, S. Osindero, Y. Teh, A fast learning algorithm for deep belief nets, Neural Comput. 18 (2006) 1527–1554.
[17] U. Fiore, F. Palmieri, A. Castiglione, A. De Santis, Network anomaly detection with the restricted Boltzmann machine, Neurocomputing 122 (2013) 13 {23.
[18] M.A. Salama, H.F. Eid, R.A. Ramadan, A. Darwish, A.E. Hassanien, Hybrid intelligent intrusion detection scheme, Soft Computing in Industrial Applications, Springer, Berlin Heidelberg, Berlin, Heidelberg, 2011 293{303.
[19] B. Dong, X. Wang, Comparison deep learning method to traditional methods using for network intrusion detection, in: Proceedings of the Eigth IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, 2016, pp. 581–585.
[20] L. Zamparo, Z. Zhang, Deep Autoencoders for Dimensionality Reduction of High-Content Screening Data, 2015, *CoRR*, abs/1501.01348.
[21] A. Dawoud, S. Shahristani, C. Raun, Software-defined network controller security: empirical study, in: Proceedings of the International Conference on Information Technology and Applications (ICITA), 2017.
[22] R. Klöti, V. Kotronis, P. Smith, OpenFlow: a security analysis, in: Proceedings of the Twenty-First IEEE International Conference on Network Protocols (ICNP), Goettingen, 2013, pp. 1–6.
[23] AliA. Ghorbani, Wei Lu, Mahbod Tavallaee, Network Intrusion Detection and Prevention Concepts and Techniques, Springer, US, 2010.
[24] M. Tavallaee, E. Bagheri, W. Lu, A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in: Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009 1,6 (2009), doi:10.1109/CISDA.