Preprocessing and Framework for Unsupervised Anomaly Detection in IoT: Work on Progress

Kurniabudi
Department of Computer Engineering
STIKOM Dinamika Bangsa
& Faculty of Engineering
Universitas Sriwijaya
Indonesia
kbudiz@yahoo.com

Benni Purnama
Department of Information System
STIKOM Dinamika Bangsa & Faculty of Engineering
Universitas Sriwijaya
Indonesia
bennipurnama@stikom-db.ac.id

Sharipuddin
Department of Computer Science
STIKOM Dinamika Bangsa & Faculty of Engineering
Universitas Sriwijaya
Indonesia
sharip_udin@yahoo.co.id

Deris Stiawan
Faculty of Computer Science
Universitas Sriwijaya
Indonesia
deris.stiawan@gmail.com

Darmawijoyo
Faculty of Mathematics and Natural Sciences
Universitas Sriwijaya
Indonesia
darmawijoyo@yahoo.com

Rahmat Budiarto
College of Computer Science & IT
Albaha University
Saudi Arabia
rahmat@bu.edu.sa

***Abstract* – A robust increasing on smart sensors in Internet of Thing (IoT) results huge and heterogenous data and becomes a challenge in data prepocessing and analysis for anomaly detection. The lack of IoT publicly available dataset is one issue in anomaly detection research. To resolve that problem, a testbed topology is proposed in this research. In addition, a high-dimensionality data analysis faces a computational complexity. The purpose of this study is to presents a global framework for anomaly detection in IoT and proposes a distributed preprocessing framework. Unsupervised learning approach has been chosen to reduce dimensionality of IoT data traffic.**

Keywords—IoT, anomaly detection, feature extraction, feature selection, unsupervised learning.

I. INTRODUCTION

In IoT network many smart objects are interconnected and communicate each other to exchange information [1]. This IoT network produces heterogenous big data to store, to process, and to present in seamless, efficient, and easy way to understand [2]. IoT has been applied in many application domains such as : Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Supply Chain Management (SCM), smart-society, cloud services, social computing and security. IoT plays an important role in daily human lives [3]. Besides, people health-care, collecting the environmental pollution data and informing them to people are also vital. The information include dangerous gases, carbon monoxide, sulfur di-oxide, humidity, wind speed and water level on a river or dam, etc. [4]. By increasingly a number of sensor in IoT, anomaly detection in sensor traffic become more important [5].

Even though anomaly detection researches have been done in many fields, anomaly detection in IoT still faces a lot of problems such as: false alarm, detection rate[6][7], high dimensionality[8][9], computational complexity[10][11] and computational time[12]. Some researches have been done to resolve that problems. A work by Fernandes et al. [13], discusses anomaly detection mechanisms based on statistical procedure Principal Component Analysis (PCA) and Ant Colony Optimization metaheuristic. Then the authors use modified Dynamic Time Warping metrics to identify anomalies. The authors claim a satisfactory level of false alarm rate results. However, limited flow attribute are used in their research. Alipour et al. [14] use supervised learning and anomaly based behavioral analysis technique that build statistical metric known as *n-gram* to detect deviations from normal behaviors. The experiment results show a low false alarm and high detection rate. Nevertheless, they research only detect attacks on IEEE 802.11 network traffic, as we now IoT traffic is not a homogeneous network. In high-dimensional data, researcher need to combine an unsupervised feature extractor with anomaly detector. While 1-support vector machines (1-SVM) is effective in learning feature vector but lack in high-dimensional data, Dynamic Bayesian Network (DBN) is used to handle it [9]. Authors in [11] optimized feature by a linear canonical correlation approach. Next, from the selected optimal features, the feature association impact scale is explored. The experiment result show that feature correlation decreases the computational and time complexity. Many works are able to maintain detection accuracy with lower computational complexity and time; however, they are not yet tested on a real IoT dataset due to the limited publicly available IoT dataset [15].

On the other hand, data preprocessing and analysis play an important role in anomaly detection research. According to [16], data preprocessing is the important phase in anomaly detection. On discovery knowledge task such as identifying abnormal data, data prepocessing is needed. Data that collected from smart sensor will be processed for many purposes, one of them is to mining knowledge[17]. Many researches do not mention in detail about data preprocessing. So, it is difficult to understand how data are prepared for learning phase. This paper is aimed to presenting the data preprocessing phase and analyzing data.

The rest of paper is organized as follows: In section 2, we presents a brief relevant theory and research in anomaly detection and data preprocessing. In section 3 the common anomaly detection phase is described. In section 4 the proposed framework for anomaly detection in IoT introduced. Section 5 proposes a testbed topology. Lastly, Section 6 presents the conclusion and future work.

II. RELEVANT THEORY

A. Anomaly Detection in IoT

In the recent years, anomaly detection has become a major research topic. Anomaly detection is a type of Intrusion Detection System (IDS). As mentioned in

978-1-5386-5721-8/18/$31.00 ©2018 IEEE

[8],[18],[19] IDS can be categorized as signatured-based and anomaly-based detection. In both types of IDS, the system tries to identify any anomalous patterns form traffic stream. If an abnormal pattern found, the alarm will triggered. This approach can be used to detect any unknown attacks or nowaday attacks.

TABLE I. SUMMARY OF ANOMALY DETECTION IN IOT

Author	Mechanism	Algorithm	Dataset	Type of anomaly	Output
(Ahmad *et al.*, 2017)[5]	Done by calculate prediction error and an anomaly likelihood measure computation	Hierarchical Temporal Memory(HTM)	NAB dataset	Spatial and Temporal	Numenta Anomaly Benchmark (NAB) Score
(Nesa *et al.*, 2017)[20]	Sensor data, preprocesing, detect error, detect event	Sequence based learning algorithm : Influential Relative Grade (IRG) and Relative Mass Function (RMF)	Laboratory setup dataset, 8 UCI Dataset, DAPHNet	Error and Event	Accuracy (Ac), Recall (Re), False Positive Rate (FPR), Precission (Pr), Specificity (Sp)
(Bostani & Sheikhan, 2017)[21]	Identifying malicious nodes, anomaly detection (mapreduce), anomaly detection decision based on a voting mechanism	optimum-path forest algorithm	Simulation	Insider attack: sinkhole and selective forwarding	True Positive Rate (TPR), False Positive Rate (FPR), and Accuracy Rate (AR) of
(Diro & Chilamkurti, 2017)[22]	Encode feature, compared distributed training and centralized.	Deep Learning	NSL-KDD	Attacks :DoS, Probe, U2R and R2L	Accuracy, Detection Rate, False Alarm Rate,
(Domb *et al.*, 2017)[23]	Data collection & cleansing, pattern recognition, rules contraction, rules evaluation, integrity & completeness, simulation & testing, deployment	Basic method combined with Random- Forest (RF)	Prototype of an IoT environtment	Rule violation	RF building time, Combined Factor, Classification time, Accuracy
(Bosman *et al.*, 2017)[24]	Analize neighborhood characterization, measure neighboorhood size, analize detection performance	Unsupervised machine learnig	GSB, Intel Barkeley, Indoor WSN (testbed)	Anomaly sensor	Precission, Recall, F-Measure

Many works have ben done in anomaly detection, especially related to data communication networks. For example, Tartakovsky et al. [25] resolve issue of rapid anomaly detection in computer network traffic by proposing statistical approach named as sequential change point detection. Their experiment results confirmed that the proposed method has better perfomance with low false alarm. Oreilly et al.[26] conduct a research on a distributed anomaly detection scheme. Minimum Volume Elliptical PCA (MVE-PCA) applied in this approach. Evaluation result show superior performance of the propose scheme. Beside statistically, another method has been used by researcher is machine learning algorithm. Such as research done by Singh *et al.* [27], a random forest algorithm has proposes to reslove issues when detecting treath with larges dataset. The result algorithm outperform another machine learning algorithm. On research G. Pachauri & S. Sharma [28], a machine learning algorithm implemented to resolve the problem with anomaly and fault detection on wide range wireless sensor network. The experiment result show the proposes framework perform quickly, accurately and low false alarm ratio in detectiong fault sensor. Even though the algorithms used by researchers vary, as mentioned in[29], unsupervised learning algorithm highly improve the accuracy detection rate of anomaly detection of supervised algorithm.

As we know the anomaly detection research is mature field especially in WSN, but still limited in case of IoT. Table 1 show summary of anomaly detection research in IoT.

B. Data Preprocessing in Anomaly Detection

Summeet and Xian stated in [30] "*Data preprocessing prepares input data for pattern learning by reducing noises and normalizing, selecting, and extracting features*". Thus, data preprocessing is important step in data analysis. Acording to Davis and Foo [31] Machine Learning Algorithm cannot generally be applied to raw data. So raw data must be preprocessed. Data preprocessing transforms data traffic to series that will be called as feature.

The purposes of data preprocessing is to prepares input data that will use for pattern learning by removing irrelevant data, normalizing data, and selecting and extracting features. We use same term for output measurement such as terms of accuracy, detection rate and false alarm rate. The common mechanism used by researchers are summarized in Table 1.

Researches in anomaly detection have been done for long time, and it is indicated by the emergence of paper surveys in anomaly detection studies. However there are very limited papers that discuss preprocessing and analysis of data on anomaly detection. Thus, it motivates us to work on the data preprocessing and analysis and potentially contribute the following.

- A theoretical framework of anomaly detection in IoT.
- A testbed topology for anomaly detection in IoT.
- An unsupervised anomaly detection framework in IoT.
- A distributed preprocessing phase for anomaly detection in IoT.

III. ANOMALY DETECTION PHASE

In this section we will disscus anomaly detection phase. Fig. 1 shows the common framework for anomaly detection in IOT. There are four phase in common anomaly detection framework, includes : capturing data, feature extraction, feature selection and anomaly detection.

A. Data Capture

The first phase of anomaly detection is data collection. From data that present in table 1. previous researcher use public dataset such as : NAB, 8 UCI Dataset, DAPHNet, KDD, and Inter Berkeley. Others using laboratory setup, simulation or testbed topology. Usually this dataset contains raw data in the form of pcap file. In this research we collecting data sensor from simulation topology.

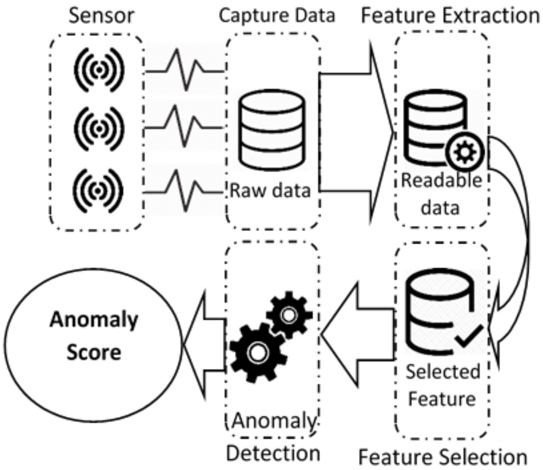

Fig. 1. Common Anomaly Detection Phase

B. Feature Extraction

Feature extraction techniques are used to extract a feature set from original feature set. Feature extraction can be used to reduce dimensionality and simplify presentation of data. Principle Component Analysis (PCA) is the most used [32]. Reducing dimentionality of data will decrease computational cost.

C. Feature Selection

Feature selection is an important phase in anomaly detection approach, used for reducing computational complexity, identifying relevan feature, cleaning data and improving the accuracy of detection algorithm [33]. Feature selection method is used to select a subset of relevant feature from the full set of feature and it is done to minimize an irrelevant feature. An Irrelevant feature induces computational cost.

D. Anomaly Detection

Methods and approaches have been widely developed by researchers and almost all of the studies use same output measurements, such as : Accuracy (Ac), Detection Rate (DR), and False Alarm Rate (FAR), as shown in Table 1. Acording to Ahmed et al. [34], there are very limited universal anomaly detection methods. Not all of the succesful methods on wired can be implemented in wireless network.

IV. Proposed Frameworks

This paper proposes two frameworks: global framework and preprocessing framework. The proposed global framework is modified from the work by Druba And Jugal [35]. The proposed prepocessing framework is a distributed framework.

A. Global Framework

Fig. 2 illustrates the proposed global framework. There are five phases in the proposed global framework as follows.

1) *Building topology*: for dataset creation purpose, we build a tesbed topology that represent smart environment, as described in the previous section.

2) *Sniffing packet from sensor*: TCPdump has been chosen to collect data on the middleware. On the other side we use Wireshark to capture data on the server. The data captured from these sensors are in raw data form and stored in pcap file. Then, these raw data are passed to the preprocessing phase.

3) *Preprocessing*: this phase plays an important role. Preprocessing step such as dimensionality reduction will remove irrelevant and redundant data, increase learning accuracy and improve result. There are two mechanisms in this phase: feature extraction and feature selection phase. More detail on the preprocessing will be discussed in distributed preprocessing framework section.

4) *Learning*: In this phase an unsupervised machine learning technique will be choosen.

5) *Scoring and labeling:* we implement the best score measurement, then followed by data labeling, as normal traffic or anomaly traffic.

B. Distributed Preprocessing Framework

Many researches have proven that a distributed system shows best perfomance for anomaly detection. According to J. Comput *et al.* [36], by maximazing a distributed in-network processing in hierarchical architecture achieve an effectively and accurately classifies the data in identified anomalies. Chen et al., [37], a distributed anomaly detection is scalable for large data size. Behal et al. [38] proposes an entropy-based distributed attack detection system. Their experimental results show that the system is able to detect

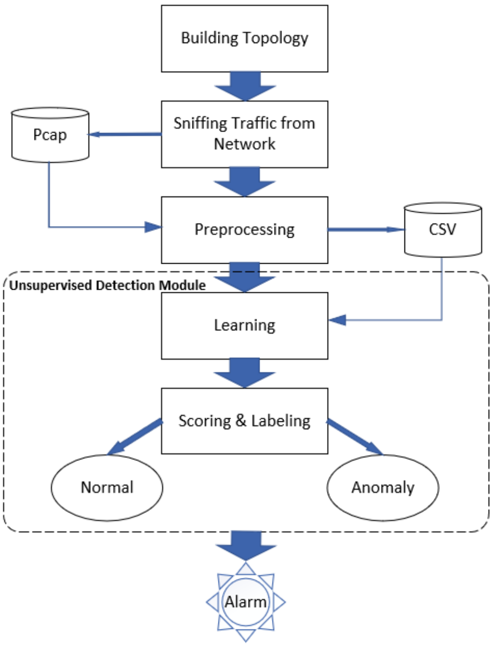

Fig.2. Anamoly Detection in IoT Framework

DDOS attack and flash event better than existing entropy-based defense system in term of detection rate, precision, f-measure, reduced FPR, classification rate.

Fig 3. presents the proposed preprocessing framework, called as distributed unsupervised preprocessing framework. The purpose of this framework is to transform data and to reduce dimentionality that will contribute to decreasing computational cost. There are two steps involve in the proposed frameworks.

1) Extract raw data: on this step, raw data were captured and stored in a database. Then will be extracted and then transformed to a readable format. Fig. 4 shows the flow chart of feature extraction from raw data file.

2) Reduce dimensional: in this step feature selection method will be implemented and effectively will contribute to dimentional reduction in designing a feature selection method. A better feature selection result will improve learning capability. Besides, the accuracy, scalability and stability must also to be considered in designing feature selection method [39]. Form this motivation, an online feature selection is chosen as a candidate to be used in this research. Feature selection methods such as Grafting, Alpha-investing, OSFS, Fast-OSFS and SAOLA will be considered to be compared to investigate the best method.

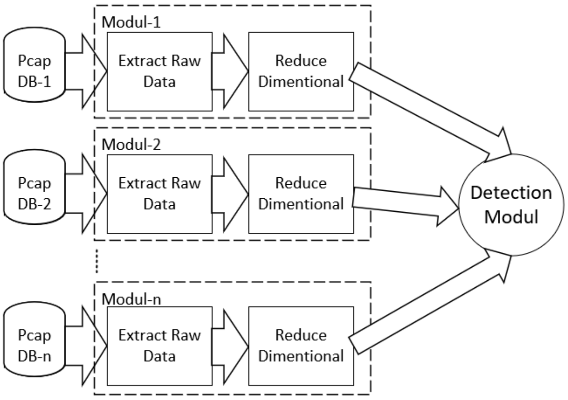

Fig. 3. Preprocessing phase

V. TESTBED TOPOLOGY

As earlier mention, one challenge in in IoT research is lack of publicly available dataset. To overcome this challenge, we set a testbed topology for creating a new dataset. The layout of the proposed testbed topology to be used in this research is shown in Fig. 5.

A. Sensor

The proposed topology represents a smart environment in an IOT system. A humidity sensor, soil moisture sensor, wind speed sensor, carbon monoxide sensor and water level sensor are deployed in the topology. Table 2 depicts the sensors used in the proposed tesbed topology.

B. Communication Protocols

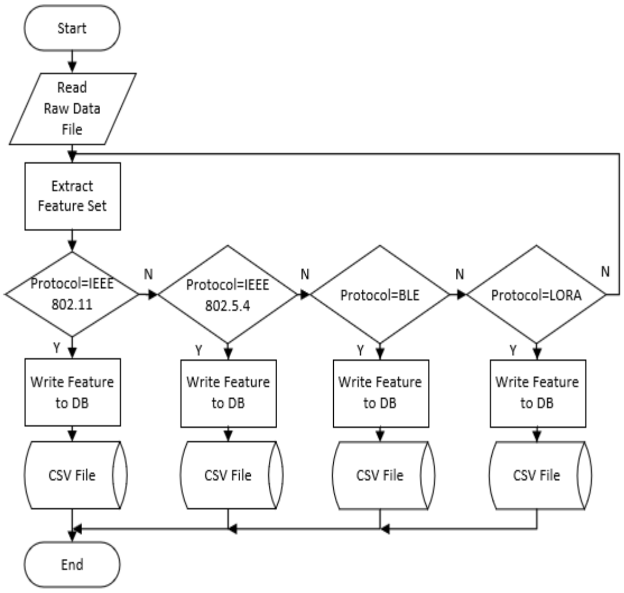

Fig. 4. Feature extraction Flowchart

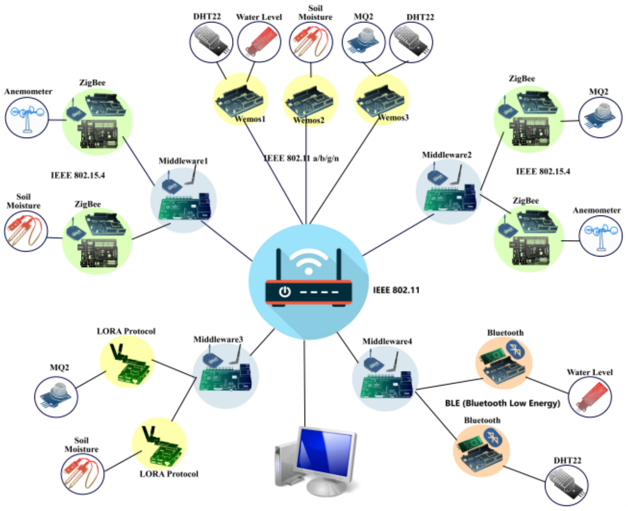

Fig. 5. Dataset Topology

As for the data communication, the proposed topology considers some wireless communication standards such as IEEE 802.15.4 for Zigbee, LoRa, IEEE 802.11 a/b/g/n for Wi-Fi and IEEE 802.15.1 for Bluetooth Low Energy (BLE). Table 3 shows the equipment used in the proposed topology.

TABLE II.The list of sensors use in topology

Sensor Name	Function	Brief Description
Anemometer sensor	for measure the speed meters/ of wind	Output : Pulse Digital TTL
Soil Moisture sensor	for measure the volumetric water content in the soil	Output: analog, 3,3 or 5 Volt
MQ2	for measure gasses and smoke	Output : analog, measure 300-10000 ppm
DHT22	for measure humidity	Output: digital , measurement range: 0-100%RH/40-80℃.
Water Level sensor	For measure level or amount of liquid	Output: analog, DC 3-5 Volt / <20mA, detection area : 40 mm x 16 mm

TABLE III.THE LIST OF MODUL USE IN TOPOLOGY

Modul Name	Parts	Specification	Protocols	Function
Middleware	Xbee Pro	Range: 30-100 meters, frequency band: 2.4 Ghz, transmit / receiver current : 45/50 mA, Channels : PAN ID, 64-bit IEEE MAC, 16 Channels	IEEE 802.5.4 (Zigbee)	Communication modul end device and middleware
	Wifi-USB moduls	USB WIFI 802.11b/g/n	IEEE 802.11b/g/n (Wifi)	Connecting wifi and zigbee
	Raspberry Pi 3	Processor: 1.2 GHz 64-bit Quad-Core CPU ARMv8, Wireless LAN, RAM : 1GB	IEEE 802.11n (Wifi)	Host on middleware
Wireless Hardware	Wireless Router	N301 Wireless Router Tenda, 1 interface 10/100 Mbps WAN, 3 interface 10/100Mbps LAN Ports	IEEE 802.11b/g/n (Wifi)	Center point, collecting packet from nodes
	Wemos D1	ESP-8266, Memori : 4 Mb Flash	IEEE 802.11b/g/n (Wifi)	As end-node on wifi modul
Bluetooth Hardware	Bluetooth low energy	v4.0 wireless 2MHz	IEEE 802.5.1 (BLE)	Wireless ommunication media with low energy
	Wemos D1	ESP-8266, Network protocol 802.11 b/g/n, Memori : 4 Mb Flash	IEEE 802.5.1 (BLE)	End node wifi modul
Wireless Protocols	Lora Shield v95	Lora Shield version 95. wireless 868MHz	LoRa	Long-range communication protocol
	Wemos D1	ESP-8266, Memori : 4 Mb Flash	IEEE 802.11 b/g/n (Wifi)	End node zigbee protocol
	I/O Expansion shield	Expansion Shield for Arduino V7 SKU:DFR0265 3.3V/5V operating voltage select	IEEE 802.5.4 (Zigbee)	Connecting arduino and xbee
	XBEE Pro	range: 30-100 meters, frequency band: 2.4 Ghz, transmit / receiver current : 45/50 mA, Channels : PAN ID, 64-bit IEEE MAC, 16 Channels.	IEEE 802.5.4 (Zigbee)	Communication modul end device and middleware

VI. CONCLUSION

The lack of universally anomaly detection techniques that can work both in wired and wireless network is one of the most challenging research in this field. As we now most of IoT devices are in wireless network. Another challenge in anomaly detection research is high-dimentionality of data that contribute to the complexity of the computational. In this paper we presented a theorical concept for anomaly detection in IoT. Although this work still in progress, from the best of our knowledge, there is no framework for anomaly detection in IoT has been proposed. As a part of the proposed framework a distributed preprocessing framework was introduced in this paper. With the lack of published dataset in IoT for anomaly detection, a testbed topology has been designed to support this research. As we now, data preprocessing is an important step in data analysis. In the most of anomaly detection researches, feature extraction and feature selection are included in data preprocessing phase. After extracting features from raw data, a proper selection of relevant features will contribute to increase the accuracy of the learning process. In future work we will conduct an experiments by comparing some online feature selection techniques to determine the most effective and relevant features.

ACKNOWLEDGMENT

This reserach supported by STIKOM Dinamika Bangsa through human resource development programs and collaboration with Comnet Lab Universitas Sriwijaya.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018.

[4] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, “Urban planning and building smart cities based on the Internet of Things using Big Data analytics,” *Comput. Networks*, vol. 101, no. 2016, pp. 63–80, 2016.

[5] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, “Unsupervised real-time anomaly detection for streaming data,” *Neurocomputing*, vol. 262, pp. 134–147, 2017.

[6] N. B. Aissa and M. Guerroumi, “Semi-supervised Statistical Approach for Network Anomaly Detection,” *Procedia Comput. Sci.*, vol. 83, no. Fams, pp. 1090–1095, 2016.

[7] A. A. Nasr, M. M. Ezz, and M. Z. Abdulmaged, “An Intrusion Detection and Prevention System based on Automatic Learning of Traffic Anomalies,” *I.J. Comput. Netw. Inf. Secur.*, vol. 1, no. 1, pp. 53–60, 2016.

[8] J. Zhang, H. Li, Q. Gao, H. Wang, and Y. Luo, “Detecting anomalies from big network traffic data using an adaptive detection approach,” *Inf. Sci. (Ny).*, vol. 318, no. August, pp. 91–110, 2015.

[9] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, “High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning,” *Pattern Recognit.*, vol. 58, pp. 121–134, 2016.

[10] A. Satoh, Y. Nakamura, and T. Ikenaga, “A flow-based detection method for stealthy dictionary attacks against Secure Shell,” *J. Inf. Secur. Appl.*, vol. 21, pp. 31–41, 2015.

[11] V. Jyothsna and V. V. Rama Prasad, “FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale,” *ICT Express*, vol. 2, no. 3, pp. 103–116, 2016.

[12] A. Juvonen and T. Hamalainen, “An Efficient Network Log Anomaly Detection System Using Random Projection Dimensionality Reduction,” *2014 6th Int. Conf. New Technol. Mobil. Secur.*, pp. 1–5, 2014.

[13] G. Fernandes, L. F. Carvalho, J. J. P. C. Rodrigues, and M. L. Proença, “Network anomaly detection using IP flows with Principal Component Analysis and Ant Colony Optimization,” *J. Netw. Comput. Appl.*, vol. 64, no. February, pp. 1–11, 2016.

[14] H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, “Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2158–2170, 2015.

[15] M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future to Internet of Things security: A position paper,” *Digit. Commun. Networks*, 2017.

[16] J. J. Davis and A. J. Clark, “Data preprocessing for anomaly based network intrusion detection : A review,” *Comput. Secur.*, vol. 30, no. 6–7, pp. 353–375, 2011.

[17] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, “Data quality in internet of things: A state-of-the-art survey,” *J. Netw.*

Comput. Appl., vol. 73, pp. 57–81, 2016.

[18] A. Juvonen, T. Sipola, and T. Hämäläinen, "Online anomaly detection using dimensionality reduction techniques for HTTP log analysis," *Comput. Networks*, vol. 91, pp. 46–56, 2015.

[19] D. Santoro *et al.*, "A Hybrid Intrusion Detection System for Virtual Jamming Attacks on Wireless Networks," *Measurement*, 2017.

[20] N. Nesa, T. Ghosh, and I. Banerjee, "Non-parametric sequence-based learning approach for outlier detection in IoT," *Futur. Gener. Comput. Syst.*, 2017.

[21] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Comput. Commun.*, vol. 98, pp. 52–71, 2017.

[22] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Futur. Gener. Comput. Syst.*, 2017.

[23] M. Domb, E. Bonchek-Dokow, and G. Leshem, "Lightweight adaptive Random-Forest for IoT rule generation and execution," *J. Inf. Secur. Appl.*, vol. 0, pp. 1–7, 2017.

[24] H. H. Bosman *et al.*, "Spatial anomaly detection in sensor networks using neighborhood information," *Inf. Fusion*, vol. 33, pp. 41–56, 2017.

[25] A. G. Tartakovsky, A. S. Polunchenko, and G. Sokolov, "Efficient Computer Network Anomaly Detection by Changepoint Detection Methods," *IEEE J. Sel. Top. Signal Process.*, vol. 7, no. 1, pp. 4–11, 2012.

[26] C. Oreilly, A. Gluhak, and M. A. Imran, "Distributed Anomaly Detection Using Minimum Volume Elliptical Principal Component Analysis," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 9, pp. 2320–2333, 2016.

[27] K. Singh, S. Chandra, A. Thakur, and C. Hota, "Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests," *Inf. Sci. (Ny).*, 2014.

[28] G. Pachauri and S. Sharma, "Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms," *Procedia Comput. Sci.*, vol. 70, pp. 325–333, 2015.

[29] S. Agrawal and J. Agrawal, "Survey on Anomaly Detection using Data Mining Techniques," *Procedia - Procedia Comput. Sci.*, vol. 60, pp. 708–713, 2015.

[30] D. Summeet and D. Xian, *Data Mining and Machine Learning in Cybersecurity*. CRC Press, 2011.

[31] J. J. Davis and E. Foo, "Automated feature engineering for HTTP tunnel detection," *Comput. Secur.*, vol. 59, pp. 166–185, 2016.

[32] S. Khalid, T. Khalil, and S. Nasreen, "A survey of feature selection and feature extraction techniques in machine learning," *2014 Sci. Inf. Conf.*, pp. 372–378, 2014.

[33] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *Ieee Commun. Surv. tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[34] Q. M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, pp. 1–13, 2015.

[35] B. Dhruba K and K. Jugal K, *Network Anomaly Detection A Machine Learning Perspective*. 2014.

[36] J. P. D. Comput, H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 790–806, 2013.

[37] P.-Y. Chen, S. Yang, and J. A. McCann, "Distributed real-time anomaly detection in networked industrial sensing systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3832–3842, 2015.

[38] S. Behal, K. Kumar, and M. Sachdeva, "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events," *J. Netw. Comput. Appl.*, 2018.

[39] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, 2018.