AFRICAN JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES

Journal website: https://journals.must.ac.ke

A Publication of Meru University of Science and Technology

Security Intrusion monitoring model for Internet of Things (IoT) using sniffing tools on wireless sensor networks

Joseph Gitonga Imathiu[1*], Amos Chege[1], Amos Omamo[1]

[1]School of Computing and Informatics, Meru *University of Science and Technology, Meru, Kenya*

ARTICLE INFO

KEYWORDS

Internet of Things (IoT

Wireless Sensor Networks (WSN

Deep Neural Network (DNN)

Denial-of-service (DoS)

ABSTRACT

The Internet of Things (IoT) has revolutionized the way devices interact and share data over wireless sensor networks (WSN), enabling seamless connectivity and automation. However, the proliferation of IoT devices has raised serious security and privacy risks concerns due to their inherent vulnerabilities. This paper proposes a model for security intrusion monitoring by analyzing the existing literature and providing insights into the design, implementation, and effective deployment of the proposed model to detect intrusion in IoT using sniffing tools for network traffic analysis in real-time within WSN. The model passively monitors network traffic and identifies anomalous patterns, unauthorized access attempts, and abnormal device behavior. The review findings highlight the significance of the proposed model in enhancing the security of IoT systems. By detecting anomalous behavior and potential security breaches. The model enables timely response and mitigation actions to ensure the confidentiality, integrity and availability (CIA) of IoT devices data. The model includes consideration of network architecture, deployment of intrusion detection algorithms, and establishment of response mechanisms. It identifies various types of security threats, such as unauthorized access attempts, Denial-of-service, Distributed DoS, Brute-force, Heartbleed, Botnet, Inside Infiltration and device tampering, thereby providing response mechanisms that include generating alerts, isolating compromised devices, or blocking suspicious network traffic. The model incorporates a feedback loop to continuously update the detection mechanisms and adapt to evolving security threats in real-time. Series of experiments and simulations to be conducted using various IoT devices and network scenarios to evaluate model effectiveness. The model to comprise of wireless Router, MatLab for Deep Neural Network (DNN) training, Raspberry Pi, Wireshark setup and an array of Internet of Things (IoT) devices. The researcher to use dataset by extracting intrinsic, host-based and time-based attributes from Wireshark Sniffing tool. The datasets generated shall be piped by tshark to an output text file saved as a csv. Under-sampling technique to be used to address class imbalance of datasets. The model shall then be trained using the dataset to be able to detect intrusion in IoTs. The results is expected to demonstrate the model's ability to detect a wide range of security intrusions with high accuracy and minimal false positives. In conclusion, the model offers a proactive approach to safeguard IoT deployment. By leveraging sniffing tools and advanced analysis techniques, the model enhances the detection and response capabilities, enabling efficient protection against emerging threats in IoT. However, challenges associated with the model are identified, including the complexity of network monitoring and potential privacy concerns

*Corresponding author: Joseph Gitonga Imathiu Email: gitimathiu@gmail.com

https://doi.org/10.58506/ajstss.v2i2.164

AFRICAN JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES ISSN :2958-0560

Introduction

Invention of Internet of Things (IoT) opened the world to a dawn of information sharing bridging the physical gap between sources and consumers of different contents. IoT has rapidly evolved into a field that involves the interconnection and interaction of smart objects, which are objects or devices with embedded sensors, on-board data processing capability, and a means of communication, to provide automated services and applications (Butun et al., 2020). Nowadays, the Internet of Things (IoT) revolution is becoming the focus of research, and both security and privacy risks are recognized as the main issues for IoT applications, mainly because of its implementation in critical areas, such as healthcare systems (Abdullah et al., 2019). There are many potential security and privacy threats to IoT, such as attacks against IoT systems and unauthorized access to private information of end users. As IoT starts to penetrate virtually all sectors of society, such as retail, transportation, healthcare, energy supply, and smart cities, security breaches may be catastrophic to the actual users and the physical world. Currently, about five billion devices has been interconnected with a prediction of having up to (50) fifty billion connected smart devices by the year 2025 (Ren et al., 2016).

As alluded by (Zhang et al., n.d.) Internet of Things (IoT) has gained significant momentum as a technology to connect physical objects to the Internet and to facilitate machine-to-human and machine-to-machine communications. Over the past two decades, IoT has been an active area of research and development endeavors by many technical and commercial communities. This showing growing trends of integration of IoT concept across most spheres of life. IoT enables integration of numerous devices, even semi-finished goods. IoT applications are designed to create real time decision-making processes by eliminating central control conditions of analysis. The novelty of this technology is that there is no need for integrated data process within standard technology. By this way, an ordinary object can evolve to an intelligent device and equipment in the smart factory can easily and rapidly communicate with the central control system (Hopali et al., 2018). IoT represents systems that are made up of real-world things and sensors connected via an internet infrastructure and as more IoT based devices increases in the network, the more the need to keep vigil to inhibit intrusions (Pundir et al., 2020).

Although IoTs ease daily activities benefiting human operations, they bring serious security challenges. IoTs have become potentially vulnerable targets for cybercriminals, so companies are investing billions of dollars to find an appropriate mechanism to detect these kinds of malicious activities in IoT networks. Nowadays intelligent techniques using Machine Learning (ML) and Artificial Intelligence (AI) are being adopted to prevent or detect novel attacks with best accuracy (Tabassum et al., 2019). It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analyzers help identify and investigate various cyber threats (Tawalbeh et al., 2020).

The privacy and security in IoTs are concerned with confidentiality, integrity, and availability of the information and/or services. Meeting these security goals is very important for modern homes to ensure trust and to guarantee the safety of data (Tabassum et al., 2019). To achieve this security and privacy in networks, professionals involved need make use of network packet sniffers to always keep an eye to the health of the networks. A Packet sniffer is used for capturing network traffic, traffic analysis and network troubleshooting. To address above issues of security and Privacy risk in IoT, the researcher aims at developing an experimental setup model that could detect intrusion.

Literature Review

Deep Learning (DL) algorithms outperform Ma-

chine Learning (ML) algorithms in applications involving large datasets. DL becomes most relevant in IoT security applications as IoT environments are characterized by the production of vast amounts and a variety of data (Khraisat et al., 2019). Furthermore, DL is capable of the automatic modeling of complex feature sets from the sample data. Another advantage of DL algorithms is their ability to allow deep linking in IoT networks. This enables automatic interactions between IoT-based systems in the absence of human intervention to perform assigned collaborative functions (Memos et al., 2022). Because of their ability to extract hierarchical feature representations in complex deep architecture, DL can be classified as a branch of ML algorithms that uses multiple non-linear layers of processing to extract feature sets. These feature sets are then used for abstraction and pattern detection after necessary transformations.

As shown in Figure1, DL can be used in a generative mode with unsupervised learning, discriminative mode using supervised learning, or a hybrid approach by combining both modes.

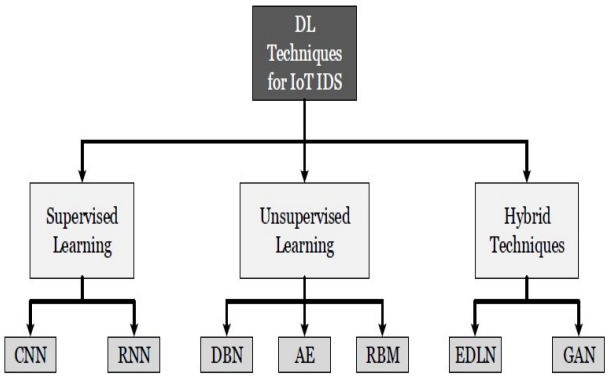

Figure1: *Taxonomy of potential Deep Learning techniques for IoT IDS*

Convolutional Neural Network (CNN)

CNN is a discriminative DL algorithm, which was designed to minimize the number of data inputs required for a conventional artificial neural network (ANN) through the use of equivariant representation, sparse interaction and sharing of parameters. Thus CNN becomes more scalable and requires less time for training. There are three-layer types in a CNN, namely convolutional layer, pooling layer and activation unit. The convolutional layers use various kernels for convoluting data inputs. The pooling layers downsize samples, thus minimizing the sizes of succeeding layers. It involves two techniques: Max pooling and average pooling, where the former chooses a maximum value for every cluster of past layers after distributing the input among distinctive clusters. The average pooling, on the other hand, calculates the average values of every cluster in the previous layer. The activation unit is able to trigger an activation function on every feature in the feature set in a non-linear fashion. CNN is best suited for highly efficient and fast feature extraction from raw data but at the same time CNN requires high computational power. Hence using CNN on resource-constrained IoT devices for their security is highly challenging. This challenge is somewhat addressed through distributed architecture where a lighter version of Deep NN is trained and implemented on-board with only a subset of vital output classes, whereas, the high computational power of the cloud is used to perform the complete the training of the algorithm. Their use in IoT environment security was discussed in previous research published in for malware detection.

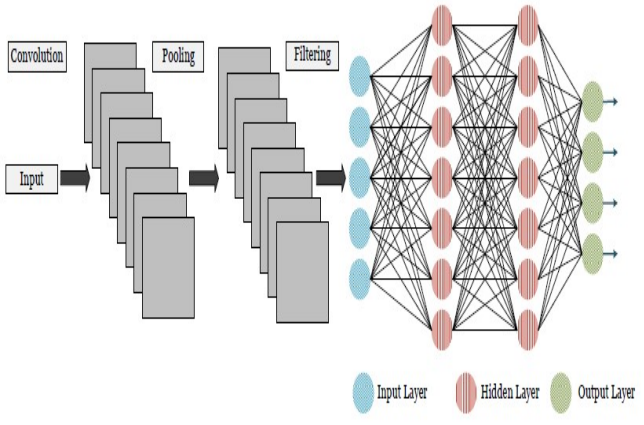

Figure 2: *Illustration of convolution neural network working*

Deep Belief Network (DBN)

Being formed by stacking two or more RBMs, DBN can be considered as unsupervised learning based

generative algorithms. They perform robustly through unsupervised training for each layer separately. Initial features are extracted in the pre-training phase for each layer, followed by a fine-tuning phase where the application of a softmax layer is executed on the top layer. It is mainly composed of two layers, i.e., visible layer and hidden layer. Though the study in discussed malicious attack detection using DBNs with comparatively better results than ML algorithms, no evidence of applicability in the IoT environment was reported in the literature.

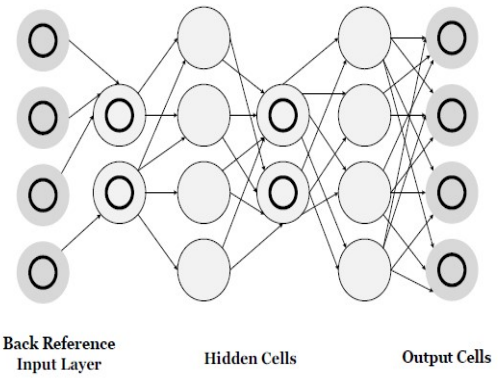

Figure 3: *Illustration of deep belief network working*

Generative Adversarial Network (GAN)

It is a hybrid DL method that uses both generative and discriminative models at the same time for training. Distributions of the dataset and samples is obtained by the generative model predictions about the authentic origination of a given sample from a training dataset and are made by the discriminative model. Both generative and discriminative models work as adversaries where the generative model attempts deception through the generation of a sample using random noise. On the other hand, the discriminative model attempts to authenticate real training data samples from deceptive samples generated by the generative model. Here, D(x) represents a binary classification giving output as real or fake (generated). The measure of correct/incorrect classification determines the accuracy and performance of both the models in an inversely proportional fashion. This results in models updating in each iteration. The study published in discussed the utility of the GAN algorithm for detecting anomalous behavior in IoT environments with promising results due to their ability to counter zero-day attacks through the generation of samples mimicking zero-day attacks, thereby causing the discriminator to learn different attack scenarios. However, the challenge with using GAN is that its training is difficult and it produces unstable results.

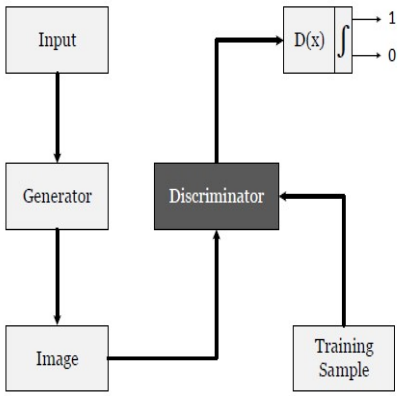

Figure 4: *Illustration of generative adversarial network (GAN)*

ANASTACIA monitoring (Advanced Networked Agents for Security and Trust Assessment in CPS /IoT Architectures)

The tool provides security monitoring services able to detect potential security breaches and attacks on cyber-physical networks. The Data Analysis component contains an anomaly-based detection tool able to detect suspect changes in the behavior of sensors. The Data Filtering and Preprocessing component receives the data from the different available monitoring agents and provides an initial pre-processing and aggregation. The Incident Detector is the core comp0nent of the module. It collects and analyzes the processed data, raising alerts once a security incident has been detected. Finally, the Attack Signatures contains the repository of attacks patterns needed for the signature-based analysis (Butun et al., 2020).

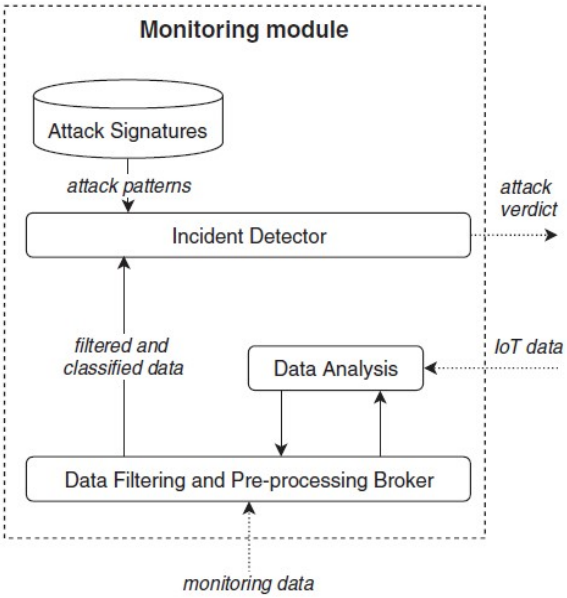

Figure 5: *ANASTACIA Monitoring Module Architecture*

Montimage monitoring tool

The MMT-IoT is a Network Intrusion Detection System (NIDS) designed and developed by the Montimage company. An NIDS is an intrusion detection system specialized in monitoring traffic to and from all devices on a network. It is capable of monitoring and analyzing the internals of a single computing system as well as the network packets passing through its network interfaces. The software is characterized by a modular architecture that provides flexibility and adaptability according to domain's requirements. IoT traffic capturing and analysis from a security perspective.

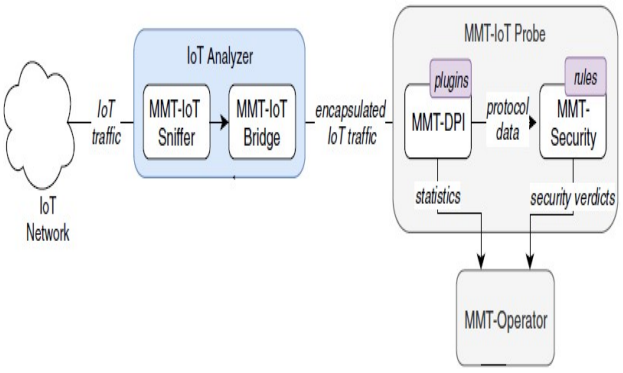

Figure 6: *Montimage monitoring tool*

Long Short-Term Memory (LSTM)

The long short–term memory (LSTM) is a type of recurrent neural network (RNN) that can classify and make predictions for temporal-dependent data such as time series datasets and signal datasets. The main attribute of LSTM based RNNs is to persist information or cell state for later use in the network. This feature makes them appropriate for performing analysis of temporal data those changes over time. Thus, LSTM networks are preferred to solve problems related to anomaly detection in time-series sequence data. Various forms of RNN, including LSTM based RNNs, have been used for anomaly and intrusion detection in IoT networks by researchers. While RNNs have demonstrated promising results in predicting time series data, the detection of anomalous traffic using these predictions is still challenging.

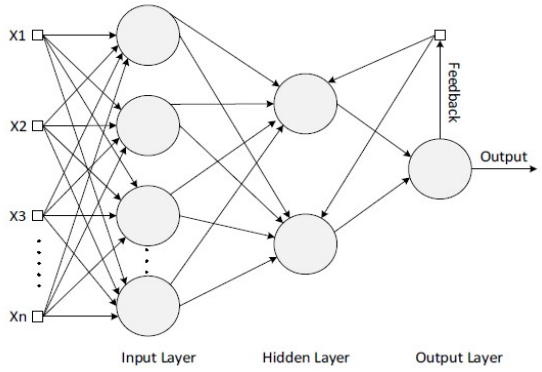

Figure 7: *Illustration of recurrent neural network algorithm*

Research proves that comparing LSTM to other algorithms such as recurrent cascade-correlation, neural sequence chunking concludes that the LSTM learns precisely compared to the other algorithms. Furthermore, lags tasks that were recurrent network algorithms in the past could not be broken down and handled using LSTM. The LSTM was introduced by Hochreiter et al and its architecture consists of the input gate, a memory cell, and an output gate. In an LSTM network, the memory cells contain the features of the LSTM network. The memory cells comprise a forget gate (ft), input gate (it), and an output gate (ot), respectively.

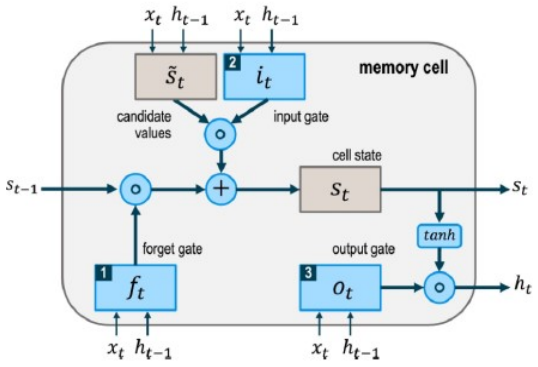

Figure 8: *LSTM block architecture*

Hybrid Intrusion Detection System (HIDS)

HIDS combines a C5 classifier and One Class Support Vector Machine classifier. HIDS combines the advantages of Signature Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS) (Memos et al., 2022)and they detect both the well-known intrusions and zero-day attacks with high detection accuracy and low false-alarm rates. The proposed HIDS is evaluated using the Bot-IoT dataset, which includes legitimate IoT network traffic and several types of attacks.

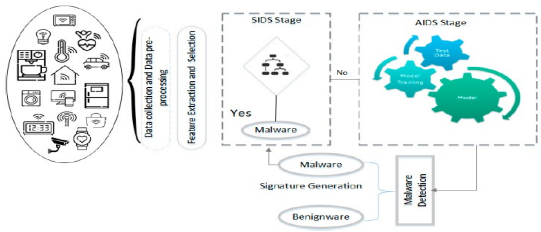

Figure 9 *: Hybrid Intrusion Detection System for the IoT ecosystem*

The proposed Model

Requirements

Comprises of wireless Router, MatLab for Deep Neural Network (DNN) training, Raspberry Pi, Wireshark Setup and an array of Commercial Internet of Things (IoT) devices.

Model experiment setup

An IoT WSN is established and extraction of intrinsic, host-based and time-based attributes dataset is done using a sniffing tool packet analyzer. Datasets generated from Wireshark will be piped by tshark to an output text file saved as a csv. Using Deep Neural Network the model is trained based on the datasets to identify different attacks. The Model is trained and evaluated a given number of times to account for any variation in data splitting and model training. Undersampling technique to be used to address class imbalance of datasets as network traffic may comprises both clean and intrusion packets.

Discussion

The model will involve the following components working together to form a cohesive Security Intrusion Monitoring Model for IoT using WSN sniffing tools to enables the detection, analysis, and mitigation of security intrusions within an IoT network, helping to ensure the integrity and security of the IoT ecosystem.

Packet Capture and Capture Engine: This component captures and stores network packets collected by the *WSN sniffing tools.* It ensures that the captured packets are preserved for further analysis. The capture engine manages the packet capture process, including filtering, buffering, and storage.

Traffic Analysis Engine: To processes the captured packets and perform analysis to identify security intrusions by applying various techniques, such as statistical analysis, anomaly detection, and pattern recognition, to detect abnormal behavior, known attack patterns, or indicators of compromise.

Intrusion Detection System (IDS): The IDS component receives information from the traffic analysis engine and applies rule-based or signature-based detection mechanisms to identify specific security intrusions. It compares the observed network traffic against a database of known attack signatures or predefined rules to identify potential security breaches or malicious activities.

Alerting and Reporting: When a security intrusion is detected, the model will generates alerts and notifications to inform administrators or security personnel. The alerting component shall trigger real-time notifications, which can be in the form of

emails, SMS messages, or system notifications. The reporting component generates detailed reports and logs summarizing detected intrusions, providing insights for further investigation and analysis.

Response and Mitigation: This component shall involves taking appropriate actions to mitigate security intrusions which may include automated responses, such as blocking or isolating suspicious devices, or initiating remediation procedures. The response and mitigation component helps prevent further damage and protect the IoT network from ongoing or future security threats.

Monitoring Dashboard and Visualization: A monitoring dashboard will provides a graphical user interface (GUI) to visualize and monitor the security status of the IoT network by presenting real-time analytics, alerts, and reports, enabling administrators to have a comprehensive view of the network's security posture. Visualization tools will help in understanding network traffic patterns and identifying potential anomalies.

Continuous Learning and Adaptation: This component will ensures that the Security Intrusion Monitoring Model evolves and adapts to changing threats and network conditions. It includes mechanisms for continuous learning from new security incidents, updating intrusion detection rules or signatures, and incorporating feedback from security analysts or administrators.

Conclusion

The literature covered showed Deep Learning is most relevant in IoT security applications as IoT environments are characterized by the production of vast amounts and a variety of data.

Secondly, DL is capable of the automatic modeling of complex feature sets from the sample data. Also DL algorithms has ability to allow deep linking in IoT networks hence enabling automatic interactions between IoT-based systems in the absence of human intervention to perform assigned collaborative functions.

Future work

More research is needed to alleviate or reduce the vulnerability of IoT devices to intrusion in order to improve on Confidentiality, Integrity and Availability of IoT resources.

References

Abdullah, A., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). *CyberSecurity : A Review of Internet of Things (IoT) Security Issues , Challenges and Techniques*. 1–6.

Azumah, S. W., Elsayed, N., Adewopo, V., Zaghloul, Z. S., & Li, C. (2021). A Deep LSTM based Approach for Intrusion Detection IoT Devices Network in Smart Home. *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 836–841. https://doi.org/10.1109/WF-IoT51360.2021.9596033

Butun, I., Österberg, P., Song, H., & Member, S. (2020). Security of the Internet of Things : Vulnerabilities ,. *IEEE Communications Surveys & Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Hopali, E., Vayvay, Ö., & Hopalı, E. (2018). *Internet of Things (IoT) and its Challenges for Usability in Developing Countries URBAN COMPETITIVENESS INDEX View project Technology and Innovation Management in Telecommunications INdustry View project Internet of Things (IoT) and its Challenges for Usa*. *2*(January), 6–9. https://www.researchgate.net/publication/322714582

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A. (2019). *A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks*.

Memos, V. A., Psannis, K. E., Lv, Z., & Member, S. (2022). A Secure Network Model Against Bot Attacks in Edge-Enabled Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *18*(11), 7998–8006. https://doi.org/10.1109/TII.2022.3162837

Pundir, S., Wazid, M., & Singh, D. P. (2020). Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment : Survey and Future Challenges. *IEEE*

Access, *8*, 3343–3363. https://doi.org/10.1109/ACCESS.2019.2962829

Ren, Z., Liu, X., & Ye, R. (2016). *Security and Privacy on Internet of Things*.

Tabassum, A., Erbad, A., & Guizani, M. (2019). *A Survey on Recent Approaches in Intrusion Detection System in IoTs*. 1190–1197.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). *applied sciences IoT Privacy and Security : Challenges and Solutions*. 1–17.

Zhang, W. E., Sheng, Q. Z., Mahmood, A., Tran, D. H., Zaib, M., Hamad, S. A., Aljubairy, A., Alhazmi, A. A. F., Sagar, S., & Ma, C. (n.d.). *The 10 Research Topics in the Internet of Things*. 2–4.