OPEN ACCESS

Jurnal Ilmiah Ilmu Terapan Universitas Jambi
Vol. 8 No. 1. June 2024, pp. 01-10 DOI. 10.22437/jiituj.v8i1.32767

Research Article

INTELLIGENT HOME IOT DEVICES: AN EXPLORATION OF MACHINE LEARNING-BASED NETWORKED TRAFFIC INVESTIGATION

Saman M. Almufti[1], Ahmed Alaa Hani[1], Subhi R. M. Zeebaree[2], Renas Rajab Asaad[1,*], Dilovan Asaad Majeed[1], Amira Bibo Sallow[3], Hawar Bahzad Ahmad[1]

[1] Department of Computer Science, Nawroz University, Duhok, Iraq
[2] Energy Engineering Department, Duhok Polytechnic University, Duhok, Iraq
[3] Department of Information Technology, Duhok Polytechnic University, Duhok, Iraq
Corresponding author email: renas.rekany@nawroz.edu.krd

Article Info

Recieved: Mar 02, 2024
Revised: Apr 12, 2024
Accepted: May 01, 2024
OnlineVersion: May 14, 2024

Abstract

In the rapidly evolving landscape of smart homes powered by Internet of Things (IoT) devices, the twin specters of safety and privacy loom large, exacerbated by pervasive security vulnerabilities. Confronted with a heterogeneous array of devices each with unique Value of Service (QoS) requirements, devising a singular network management strategy proves untenable. To mitigate these risks, device categorization emerges as a promising avenue, wherein rogue or vulnerable devices are identified and network operations are automated based on device type or function. This novel approach not only fortifies IoT security but also streamlines network management, offering a multifaceted solution to the burgeoning challenges. Recognizing the burgeoning interest in leveraging machine learning for traffic analysis in IoT environments, this study delves deep into the potential and pitfalls of such techniques. Beginning with a comprehensive framework for categorizing IoT devices, the research meticulously examines methodologies and remedies across every stage of the workflow. Key focal points include the categorization of public datasets, nuanced analysis of IoT traffic data collection methodologies, and the exploration of feature extraction techniques. Through a rigorous evaluation of machine learning algorithms for IoT device classification, the study elucidates emerging trends and highlights promising avenues for future exploration. The culmination of this investigation manifests in meticulously crafted taxonomies, offering insights into prevailing patterns and informing future research trajectories. Moreover, the study identifies and advocates for uncharted territories within this burgeoning domain, propelling the discourse forward and catalyzing innovation in IoT security and management.

Keywords: IoT Device Classification, Machine Learning, Network Traffic Analysis, Smart Home

INTRODUCTION

The Web of Things (IoT) has grown significantly over the last ten years; estimates indicate that by 2022, there will be 14.4 billion active connections, an 18% increase. IoT is defined differently by different people, but most define it as a network that includes cameras, mobile devices, industrial machines, sensors, and other devices that are linked to each other. IoT is used in smart environments to provide consumers more control and awareness of their surroundings (Alrawi et al., 2019; Abdulqadir et al., 2021; Asaad, 2021).

Even with its many advantages, the spread of IoT raises serious security and privacy issues. The three Privacy, Security, and Performance are often given priority by IoT device makers above security, which results in poor design and susceptible equipment. Inadequately protected Internet of Things devices are appealing targets for hackers who are looking for sensitive data and unauthorised access, as shown by the cases in which smart TVs were used as listening devices (Dong et al., 2020; Ma et al., 2020; Cvitić et al., 2021; Maulud et al., 2021). By inserting malicious data, hackers may use weakly protected IoT devices to not only get unauthorised access but also to initiate wider attacks targeting connected devices or other organisations. Realising how important it is to secure Internet of Things relationships, the first step is to identify susceptible devices and automatically identify devices. This makes it easier to apply access restrictions.

A one-size-fits-all approach to network management is inadequate, considering the heterogeneous QoS requirements of Internet of Things devices. Network management automation is made possible by IoT device classification, because each categorised device may be given preset rules according to its class. There are situations where terms like “device fingerprinting,” “intrusion detection,” “traffic classification,” and “device classification” are used interchangeably. While intrusion detection uses attack patterns to determine if traffic is malicious or legitimate, traffic classification includes classifying network traffic according to a variety of criteria (Nguyen, & Armitage, 2008; Meidan et al., 2017; Salman et al., 2020; Sadeeq et al., 2021). Device fingerprinting gives each instance of a device a unique fingerprint, whereas device identification more accurately classifies devices according to manufacturer or model.

IoT device classification may be achieved mostly by observing MAC addresses as a way and DHCP negotiation; however, machine learning (ML) can make this procedure more straightforward and reveal aspects of concealed network traffic (figure 1). This research investigates machine learning (ML) based network traffic analysis for IoT device classification, emphasising on all of a device's network related activities, including data particular to individual devices and applications.

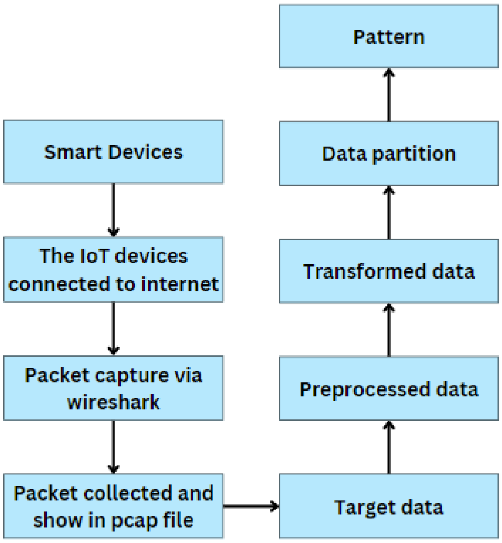
Pattern
Smart Devices
Data partition
The IoT devices connected to internet
Transformed data
Packet capture via wireshark
Preprocessed data
Packet collected and show in pcap file
Target data

Figure 1. Flowchart Of the System

The choice to focus on smart home technology was made in light of the wealth of research that is currently available, the ease of access to data, and the widespread use of Internet of Things (IoT) gadgets in smart homes. These factors highlight the importance of securing IoT devices, particularly in light of the diverse user base that varies in their level of security awareness.

LITERATURE REVIEW

The Web of Things (IoT) has grown significantly over the last ten years; estimates indicate that by 2022, there will be 14.4 billion active connections, an 18% increase. IoT is defined differently by different people, but most define it as a network that includes cameras, mobile devices, industrial machines, sensors, and other devices that are linked to each other. IoT is used in smart environments to provide consumers more control and awareness of their surroundings (Miettinen et al., 2017; Sivanathan et al., 2018; Sánchez et al., 2021; Xenofontos et al., 2021).

In order to create a thorough grasp of the topic, we carried out a thorough literature assessment by looking through publications from a variety of digital libraries as a whole including IEEE Xplore, ResearchGate, and Google Scholar, and others. Words like "IoT devices," "wearable devices," "IoT gadgets," "classification," "fingerprinting," "identification," "clustering," "classification," "travel analysis," "traffic classification," "interaction analysis," "network attributes," "network packets," "network flows," and "algorithms for learning" were among the pertinent terms that appeared in our keyword search.

We concentrated on articles published between 2018 and 2022 to make sure that latest innovations were included. We also looked through the citation and references of a few chosen papers to broaden our search. After eliminating unnecessary material from titles and abstracts, we reduced the number of papers we chose to 49 that were essential to our research. These publications were carefully examined, and those that lacked enough information on any stage of the classification procedure were eliminated.

As far as we are aware, this research is the first to investigate every one of the issues mentioned above and explain how they affect the categorization of IoT devices. To address the research questions indicated above, this survey makes the following contributions:

- A thorough analysis outlining the many uses of IoT device classification in smart homes.
- A careful analysis of the techniques used to collect data on IoT traffic.

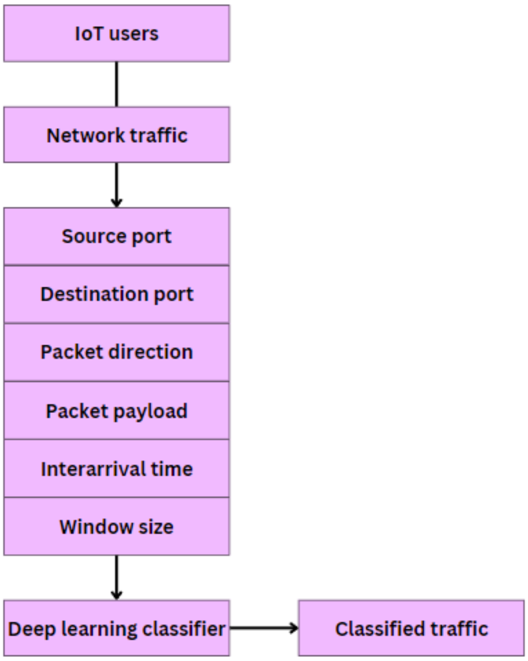

Figure 2. Approach of the system

Network and Security Management

It is quite difficult to manage the wide range of internet of things devices with a single policy. Organising each device independently and imposing network and security management policies according to its designated class is one way to tackle this problem. It's critical to discover. Attackers may be able to use these devices' weakened security to get unauthorised access to the internet or launch extensive attacks and enable DDoS assaults. Businesses' attack surface grows as a result of the Bring Your Own Device (also known as BYOD) trend, which enables workers to connect their own IoT devices to company networks. Malware on infected personal devices may spread across the network, endangering other devices. In a similar vein, the move to remote work has reduced security by bringing commercial devices into close contact with potentially weaker smart home technologies. Importantly, whitelisting which includes authorised devices is more scalable than blocking, which expands as the number of untrusted devices rises. Moreover, whitelisting makes it easier to get data from approved devices (Sivanathan et al., 2017; Perdisci et al., 2020; Ma et al., 2021). However, because hackers may imitate the behaviour of genuine devices to get beyond intrusion detection systems, it could be less effective preventing malicious assaults.

APPROACHES TO DATA ACQUISITION

This section explores the methods for gathering data that are described in the literature. We provide the results in four ways to make them easier to understand: first, we look at the devices that were taken into account for gathering data; second, we investigate the different kinds of Internet of Things (I that can be recorded; third, we talk about possible scenarios for gathering data; and fourth, we compare statistics that are accessible to the general public.

Algorithm:

```
STEP 1: Gather network traffic data generated by smart home IoT devices, including information on communication protocols, data sizes, and packet frequencies.
STEP 2: Preprocess the network traffic data by extracting relevant features such as packet headers, payload characteristics, and communication patterns.
STEP 3: Define a set of classes representing different types of smart home IoT devices, such as cameras, thermostats, or smart plugs.
STEP 4: Select appropriate machine learning algorithms, such as supervised classification or clustering, for analyzing network traffic and classifying IoT devices.
STEP 5: Train the machine learning model using labeled network traffic data to learn patterns specific to each device class.
STEP 6: Evaluate the performance of the classification model using metrics like accuracy, precision, recall, and F1-score.
STEP 7: Fine-tune hyperparameters of the machine learning algorithm to optimize classification accuracy and generalization ability.
STEP 8: Validate the trained model on unseen network traffic data to assess its ability to accurately classify IoT devices in real-world scenarios.
STEP 9: Integrate the classification model into network security systems to enhance device identification and anomaly detection capabilities.
STEP 10: Continuously update the classification model as new types of IoT devices emerge or communication patterns evolve, ensuring ongoing effectiveness in smart home environments.
```

The Classified Devices

The Internet of Things device classification procedure is based on a list of devices that need classification divided into Internet and non-IoT devices, which are made for particular and specialised purposes. On the website, a thorough inventory of well-liked Internet of Things smart home devices is updated often. Furthermore, in smart home contexts, non-IoT devices like computers, Android tablets, and cell phones coexist. It is essential to take into account both IoT and non-IoT devices while gathering traffic statistics (Shaikh et al., 2018; Marchal et al., 2019; Tahaei et al., 2020). It's important to remember, too, that classifying these disparate devices presents difficulties, in part because IoT traffic is smaller and sparser than non-IoT data.

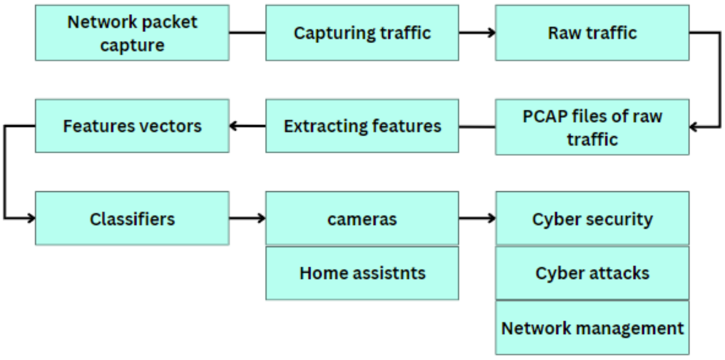

Figure 3. Workflow Methodology of the System

The Different Types of IoT Traffic

Based on how they work, Internet of Things devices produce three different kinds of traffic: i) setup traffic, which is created during installation and is also known as authorization or enrollment; ii) interacting traffic, which is created user or its environment; and iii) idle traffic, which is created when a device is not being stimulated externally (figure 3). Keep-alive or heartbeat signals, as well as frequent contacts between the electronic gadget and the software server, are examples of idle traffic.

FEATURE EXTRACTION METHODOLOGIES

The methods for feature extraction are examined in this part, including automated deep learning-based feature extraction as well as packet-level and stream-level approaches. It also provides an overview of feature dimensionality reduction methods. Data packets must be separated and transferred as part of network traffic, which is the amount of data sent across a network. These packets are then put back together by the receiving computer or device. When analysing network traffic, two methods are used: packet-level and flow-level extraction of characteristics techniques. The methods in each category are presented in the following sections, which attempt to provide a thorough rundown of these approaches.

Open-Source Feature Extraction Tools

The literature review in this part covers the current feature extraction tools. These utilities create text-based data files with feature vectors as their output after receiving network traffic that has been packet-captured in pcap format using a packet capture tool. A feature vector is created from each observation. Joy uses actual network flows, concentrating on the application levels, to extract characteristics. The sequence of IP packet arrival times and lengths, TLS record introductory lengths and timings, and other unencrypted TLS data, such as the list of recommended and selected ciphersuites, DNS addresses, telephone numbers, TTLs, and HTTP header elements, are among the salient features (Shahid et al., 2018; Hafeez et al., 2019; Meidan et al., 2020).

Features Dimensionality Reduction For Better Classification

Decreasing the dimensionality of features serves to lower computing costs while enhancing classification accuracy. This pre-processing stage identifies relevant traits and eliminates superfluous or unnecessary ones. Interestingly, in the categorization of IoT devices, feature reduction dimensionality is not frequently employed. This step is utilized in only 30% of the evaluated publications. The rationale behind this is that feature reduction is deemed unnecessary, given that the majority.

CLASSIFICATION

Building a model for multi-class classifiers is difficult because each time a new class is introduced or an existing device type's behaviour changes, the model has to be completely retrained. On the other hand, creating a classifier specifically for each device eliminates the need for costly relearning whenever a new device type is added. Since samples rejected by the categorization algorithms may be identified as distinct device kinds, this methodology also offers the option of finding other devices. Another benefit of this approach is its interpretability. Choosing one classifier per class, particularly when handling a large number of characteristics, yields a set of interpretable models rather than a single complicated model.

Nevertheless, since the results of many classifiers must be computed, one-class classifier systems have a larger computational cost. Delays may also be introduced while addressing conflicts when a sample matches several kinds of devices (figure 4). According to the research, tiebreaks take up a large amount of the time needed to identify the kind of device. Moreover, classifier performance may be impacted by unbalanced training datasets. To solve this problem, under- and oversampling strategies might be used.

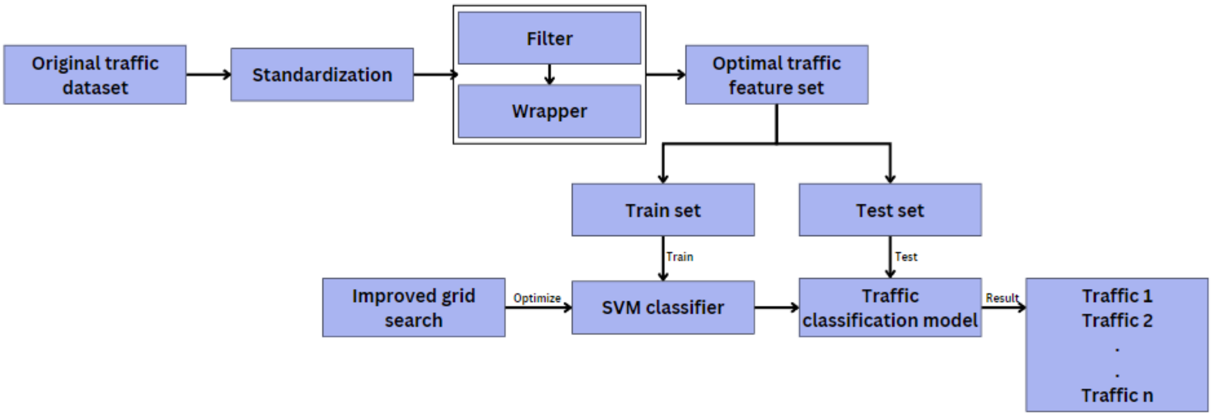

Figure 4. Implementation of the System

DISCUSSIONS AND KEY RESEARCH DIRECTIONS

We investigate lines of inquiry that haven't gotten a great deal in the field of research. Drawing on the paper's premise, it covers issues with data collecting, extracting features, and the application of machine learning.

The Imbalances Collection Problems

This is a prevalent challenge in numerous machine learning applications, and it becomes notably troublesome in IoT device categorization due to the erratic behavior of these devices (Almufti et al., 2021; Lueth et al., 2022). Certain devices, such as plugs, generate minimal data, while others, like cameras, produce extensive communication. Identifying devices belonging to minority classes becomes challenging. During the training phase, solutions based on data augmentation can be explored. It is crucial to avoid biases when overrepresenting minority classes. Striking a balance is essential to prevent overfitting of the model.

Lowering The Image Transfer Fee

Their findings indicate that an accuracy nearly identical to that achieved with all features can be attained with a restricted set of highly impactful features. It is important to highlight that while utilizing fewer features reduces the cost of feature extraction, it may also heighten the susceptibility of the classification method to malicious attacks. An attacker might find it easier to replicate the behavior of a specific IoT device and deceive the classifier by creating traffic resembling the values obtained by a single feature (Ageed et al., 2021). However, crafting traffic that simultaneously matches the values of multiple features is more complex, making it more challenging to evade a classifier considering a range of features.

Heightening the reading pace

The Necessity Of Constant Education

The dynamic nature of device behaviour and the ever-evolving IoT ecosystem necessitate frequent updates to classification models to accommodate current data patterns. To ensure the relevance of machine-learned models over time, it is imperative to explore continuous learning in machine learning pipelines. Approaches that involve training individual classification algorithm models for each device offer greater adaptability for regular retraining.

Scarcity of Labeled Data

An alternative solution involves the generation of labeled synthetic data, such as through the use of generative adversarial networks (GANs). GANs have the capability to create synthetic data that closely resembles Obtain the actual distribution of the training data by capturing the distribution of hidden classes. Train the classifier using these additional synthetic data points enhances their generalization ability.

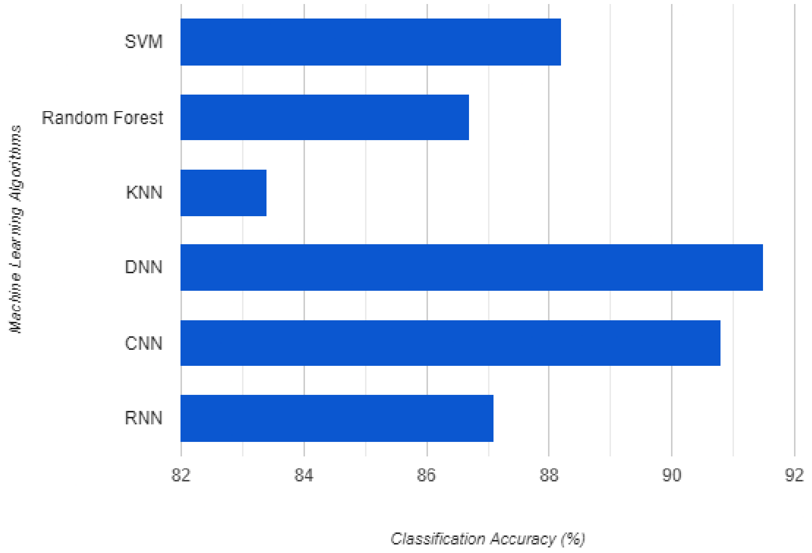

Figure 5. Classification Accuracy of ML Algorithm for Smart Home Iot Devices Classification for the System

DISCUSSING SCALABILITY

Creating scalable solutions is imperative given the exponential surge in both the quantity and diversity of IoT devices. Moreover, the emergence of edge computing introduces the intriguing possibility of leveraging the robust processing and storage capabilities provided by nearby edge servers to enhance the speed and scalability of IoT device categorization.

Table 1. System Feature and Their Description, Benefits and Challenges

Feature	Description	Benefits	Challenges
Data Acquisition:	Captures network traffic information from smart home devices using network sniffers, traffic monitors, or embedded agents.	Provides rich data for analysis, including packet headers, payload information, and communication patterns.	Limited access to data due to privacy concerns and network encryption. potential impact on network performance.
Feature Engineering:	Extracts relevant features from network traffic data such as packet size, protocol type. inter-arrival time, and communication frequency.	Enables effective machine learning model training and accurate device classification.	Selection of informative features depends on specific devices and classification goals, computational complexity of feature extraction.
Machine Learning Algorithms:	Utilizes various algorithms, including supervised (Support Vector Machines, Random Forests) and unsupervised (k-Means, clustering) methods, depending on the availability of	Offers flexibility in choosing the most suitable algorithm for specific tasks and datasets.	Model selection, tuning, and training require expertise, potential for overfitting or

Feature	Description	Benefits	Challenges
	labeled data		underfitting depending on data size and complexity.
Performance Evaluation:	Assesses the accuracy, precision, recall, and F1-score of the classification model using metrics relevant to the application.	Provides insights into model effectiveness and identifies areas for improvement.	Choosing appropriate evaluation metrics based on the classification task, ensuring data quality and representativeness for reliable evaluation.
Privacy-Preserving Techniques:	Implements techniques like data anonymization differential privacy, or federated learning to protect user privacy while still enabling device classification.	Mitigates privacy concerns and fosters user trust in the system.	Potential impact on data quality and accuracy, increased complexity and computational overhead of privacy-preserving methods.

Mud and Standardization

Another way to classify and identify IoT devices is to use Manufacturer's Usage Descriptions (MUDs). MUD is a standard established by the IETF that allows IoT device manufacturers to publish device specifications that include targeted communication patterns. IoT devices typically perform specific functions with different communication patterns, so these can be captured formally and concisely in his MUD profile (Sivanathan et al., 2018; Ageed et al., 2021; Asaad et al 2021; Yazdeen et al., 2021). Unfortunately, the adoption of his MUD specifications and mechanisms by current IoT manufacturers remains limited.

CONCLUSION

Proposing IoT device classification as a potential solution for securing and managing the IoT ecosystem, this study aimed to address key research questions through a comprehensive literature review: We showed that collecting traffic data from both IoT and non-IoT devices in a smart home is more practical considering their coexistence. His three operating modes of the device (setup, idle, interaction) were examined. Although idle and interaction modes generate large and extensive traffic, capturing setup traffic is stable but difficult due to the infrequent initialization phase. It was highlighted that the collection of traffic from outside the home reflects a real-world use case for his IoT device classification, which is often not fully explored in the literature. Additionally, bias has been identified in public datasets. it describes feature extraction approaches, focusing on the scalability and cost-effectiveness of extracting features from streams rather than packets. I guessed. Various strategies for partitioning traffic (e.g., by time interval, by number of packets, by connection, etc.) have been considered. It was noted that it is important to establish optimal parameters for flow sharing, such as: For example: number of time slots or packages. The most discriminatory features were identified and how they were calculated was discussed.

The analysis in revealed that building a multi-class classifier is not scalable and non-evolutionary and recommended building one classifier for each device type. This approach reduces retraining costs, enables the discovery of new types of instruments, and increases interpretability. The computational requirements of single class classification methods are recognized. The potential of unsupervised learning, especially to minimize labeling costs in the face of increasing device diversity, was highlighted but noted to be underexplored in the literature. The need for additional evaluation scenarios and indicators for realistic evaluation was highlighted.

ACKNOWLEDGMENTS

Thank you to all colleagues who have helped, so that this research can be carried out and completed.

AUTHOR CONTRIBUTIONS

Author 1-2 creates articles and creates instruments and is responsible for research, author 3-4 Analyzes research data that has been collected, author 5-6 assists in research data analysis and instrument validation, author 7 helps input research data.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Abdulqadir, H. R., Zeebaree, S. R., Shukur, H. M., Sadeeq, M. M., Salim, B. W., Salih, A. A., & Kak, S. F. (2021). A study of moving from cloud computing to fog computing. *Qubahan Academic Journal*, *1*(2), 60-70. https://doi.org/10.48161/qaj.v1n2a49

Ageed, Z. S., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Yahia, H. S., Mahmood, M. R., & Ibrahim, I. M. (2021). Comprehensive survey of big data mining approaches in cloud systems. *Qubahan Academic Journal*, *1*(2), 29-38. https://doi.org/10.48161/qaj.v1n2a46

Ageed, Z. S., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Rashid, Z. N., Salih, A. A., & Abdullah, W. M. (2021). A survey of data mining implementation in smart city applications. *Qubahan Academic Journal*, *1*(2), 91-99. https://doi.org/10.48161/qaj.v1n2a52

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019, May). Sok: Security evaluation of home-based iot deployments. In *2019 IEEE symposium on security and privacy (sp)* (pp. 1362-1380). IEEE.

Almufti, S. M., Marqas, R. B., Nayef, Z. A., & Mohamed, T. S. (2021). Real time face-mask detection with arduino to prevent covid-19 Spreading. *Qubahan Academic Journal*, *1*(2), 39-46. https://doi.org/10.48161/qaj.v1n2a47

Asaad, R. R. (2021). Review on Deep Learning and Neural Network Implementation for Emotions Recognition. *Qubahan Academic Journal*, *1*(1), 1-4. https://doi.org/10.48161/qaj.v1n1a25

Asaad, R. R., & Abdulhakim, R. M. (2021). The Concept of Data Mining and Knowledge Extraction Techniques. *Qubahan Academic Journal*, *1*(2), 17-20. https://doi.org/10.48161/qaj.v1n2a43

Cvitic, I., Perakovic, D., Perisa, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3179-3202.

Dong, S., Li, Z., Tang, D., Chen, J., Sun, M., & Zhang, K. (2020, October). Your smart home can't keep a secret: Towards automated fingerprinting of iot traffic. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (pp. 47-59).

Hafeez, I., Antikainen, M., & Tarkoma, S. (2019, March). Protecting IoT-environments against traffic analysis attacks with traffic morphing. In *2019 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)* (pp. 196-201). IEEE.

Lueth, K. L., Hasan, M., Sinha, S., Annaswamy, S., Wegner, P., Bruegge, F., & Kulezak, M. (2022). State of IoT—spring 2022. *IoT Analytics market report*.

Ma, X., Qu, J., Li, J., Lui, J. C., Li, Z., & Guan, X. (2020, July). Pinpointing hidden IoT devices via spatial-temporal traffic fingerprinting. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications* (pp. 894-903). IEEE.

Ma, X., Qu, J., Li, J., Lui, J. C., Li, Z., Liu, W., & Guan, X. (2021). Inferring hidden iot devices and user interactions via spatial-temporal traffic fingerprinting. *IEEE/ACM Transactions on Networking*, *30*(1), 394-408.

Marchal, S., Miettinen, M., Nguyen, T. D., Sadeghi, A. R., & Asokan, N. (2019). Audi: Toward autonomous iot device-type identification using periodic communication. *IEEE Journal on Selected Areas in Communications*, *37*(6), 1402-1412.

Maulud, D. H., Zeebaree, S. R., Jacksi, K., Sadeeq, M. A. M., & Sharif, K. H. (2021). State of art for semantic analysis of natural language processing. *Qubahan academic journal*, *1*(2), 21-28. https://doi.org/10.48161/qaj.v1n2a44

Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y., & Shabtai, A. (2020). A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Computers & Security*, *97*, 101968.

Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017, June). Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 2177-2184). IEEE.

Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*.

Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE communications surveys & tutorials*, *10*(4), 56-76.

Perdisci, R., Papastergiou, T., Alrawi, O., & Antonakakis, M. (2020, September). Iotfinder: Efficient large-scale identification of iot devices via passive dns traffic analysis. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 474-489). IEEE.

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7. https://doi.org/10.48161/qaj.v1n2a36

Salman, O., Elhajj, I. H., Kayssi, A., & Chehab, A. (2020). A review on machine learning–based approaches for Internet traffic classification. *Annals of Telecommunications*, *75*(11), 673-710.

Sánchez, P. M. S., Valero, J. M. J., Celdrán, A. H., Bovet, G., Pérez, M. G., & Pérez, G. M. (2021). A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. *IEEE Communications Surveys & Tutorials*, *23*(2), 1048-1077.

Shaikh, F., Bou-Harb, E., Crichigno, J., & Ghani, N. (2018, June). A machine learning model for classifying unsolicited IoT devices by observing network telescopes. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 938-943). IEEE.

Shahid, M. R., Blanc, G., Zhang, Z., & Debar, H. (2018, December). IoT devices recognition through network traffic analysis. In *2018 IEEE international conference on big data (big data)* (pp. 5187-5192). IEEE.

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2017, May). Characterizing and classifying IoT traffic in smart cities and campuses. In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 559-564). IEEE.

Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2018). Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, *18*(8), 1745-1759.

Sivanathan, A., Gharakheili, H. H., & Sivaraman, V. (2018, December). Can we classify an iot device using tcp port scan?. In *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)* (pp. 1-4). IEEE.

Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. *Journal of Network and Computer Applications*, *154*, 102538.

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet of Things Journal*, *9*(1), 199-221.

Yazdeen, A. A., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021). FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. *Qubahan Academic Journal*, *1*(2), 8-16. https://doi.org/10.48161/qaj.v1n2a38