International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Smart Environments IoT Device Classification Using Network Traffic Characteristics

[1]B. Srivalli, [2] Dr. G. Hemanth Kumar Yadav, [3]V.S.S.P.L. N. Balaji Lanka, [4]Dr. K. Lakshmi Devi, [5]Dr. A. Naresh, [6] P.Naresh, [7]Koppuravuri Gurnadha Gupta

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: The growing number of Internet of Things (IoT) gadgets in smart settings has made it harder to manage and protect these systems that are all linked together. Some important parts of managing IoT devices are classification and recognition. Devices can be put into groups based on how they work and behave. Using network traffic characteristics, this study suggests a way to group Internet of Things (IoT) objects in smart environments. Our method looks at the trends and characteristics of network data that IoT devices send in order to correctly identify and group these devices. This will make management easier and security better. We show testing results that show our proposed method can effectively sort different IoT devices into groups based on their network traffic signatures. We go over the trade-offs that must be made between performance, speed, and cost while implementing the categorization system in real time. Without requiring any specialised equipment or protocols, our study provides the door for operators of smart environments to monitor the existence, operation, and cyber-security of their IoT assets.

Keywords: *Traffic modeling, traffic volume, Machine learning, IoT, characteristics of network, device visibility, classification.*

1. Introduction

IoT devices that are linked to each other create "smart environments" that have changed many areas, such as home automation, healthcare, transportation, and industrial automation. Sensors, actuators, and other smart devices are built into these settings so that they can gather data, make smart choices, and automate chores. But the fast growth of IoT devices has brought about new problems, especially when it comes to managing them, keeping them safe, and making sure they can talk to each other. Classifying IoT devices correctly is a key part of solving these problems because it makes management, resource sharing, and security control much easier.

We are now living in the age of the "Internet of Things" (IoT), where more and more gadgets can connect to the internet. Internet of Things refers to the tens of billions of inexpensive devices that can communicate with distant computers and one another over the Internet on their own. It includes commonplace things like power switches, door locks, motion sensors, cameras, lights, and appliances. Sales should reach about 20 billion by 2020. [1]. Soon, thousands of IoT devices will likely be in homes, businesses, schools, and cities, creating "smart" settings that will make our lives and society better. There is, however, a big problem caused by the widespread use of IoT. It can be hard for people who run smart settings to figure out what IoT devices are tied to their network and if each one is working properly. The main reason for this is that handling an organization's assets is usually the job of several different teams working together. In a local government, for example, the facilities team might put in lighting sensors, the cleaning department might put in sewage and garbage sensors, and the local police division might put in security cameras. Coordinating with different departments to get a list of IoT assets is hard, takes a lot of time, and is prone to mistakes. This means that it is almost impossible to know exactly what IoT devices are connected to the network at any given time. Achieving "visibility" into IoT devices fast is critical for the operator, whose responsibility it is to ensure that devices are placed in the appropriate network security sections, configured for the appropriate quality of service, and able to be swiftly blocked in the event of a breach. Access is critical, as highlighted in the most recent CISCO IoT security study [2]. This is also evident from two recent incidents: vending machine assaults on a university campus network in February 2017 [4] and sensors in a fish tank that broke into a casino in July 2017 [3]. Better monitoring would have allowed the attackers to be swiftly removed from the firm network to minimise harm, and network segmentation may have prevented the attack in both scenarios.

[1]*Asst.Professor, Dept of IT, Guru Nanak Institute of Technology (A), Hyderabad*
[2] *Associate Professor, Dept of CSE, Srinivasa Ramanujan Institute of Technology (A), Ananthapuramu*
3Asst.Professor, Dept of CSE, Vignan Institute of Technology and Science (A), Hyderabad
[4] *Assistant Professor of English, Department of English and Foreign Languages, Madanapalle Institute of Technology and Science, Madanapalle*
[5]*Associate Professor, Dept of CSE, and also HOD department of MCA, Annamacharya Institute of Technology and Sciences (A), Kadapa*
[6]*Assistant Professor, Department of IT, Vignan Institute of Technology and Science(A), Hyderabad*
[7]*Asst.Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh*
* *Corresponding Author Email: rtit2009@gmail.com*

2. Related Work

This study tries to solve the problem mentioned above by creating a strong framework that accurately sorts each IoT device into a different class along with a class of non-IoT devices. Statistical attributes derived from network traffic characteristics are used to do this. The majority of IoT devices should periodically emit brief data bursts. Technically speaking, our first study in [6] was among the first to investigate the aggregate amount of traffic sent by IoT devices and the duration of inactivity before initiating a new action. We also checked how much signaling they do compared to the data flow they create. For example, we looked at how much name lookups they do with DNS and time synchronization they do with NTP. This paper adds a lot to what we've already done by using a wider range of traits on trace data collected from 28 different IoT devices over a much longer period of time (6 months).

The main goal of this work is to create a machine learning system that uses different types of network data to find and classify the normal (or baseline) behavior of IoT devices on a system. This kind of framework could be used in the future to find IoT devices that are acting strangely, possibly because of cyberattacks. However, this study does not cover any of those kinds of anomaly detection methods. This article fills in a big hole in the research on how to group Internet of Things devices based on how they send and receive data over networks.

What we're giving is:

We put 28 Internet of Things (IoT) gadgets in a living lab to make it look like a smart setting. Things like cameras, lights, plugs, motion sensors, appliances, and health monitors are among the gadgets. For 6 months, we gather and put together facts from this setting. Researchers can use a part of our data that we make public.

Furthermore, significant statistical characteristics such as cypher suites, port numbers, activity cycles, and signalling patterns are discovered. The fundamental characteristics of network traffic are made clearer by these.

Our multi-stage machine learning-based classification approach is demonstrated to be able to reliably identify individual IoT devices over 99 percent of the time based on their network behaviour.

Check how the classification system is used in real time by looking at the prices, speeds, and accuracy of the classifier.

Despite the significance of the aforementioned studies, none of them provide a thorough categorization and description of IoT devices in smart settings such as homes, cities, schools, or businesses. In addition, mathematical models aren't being made that let IoT devices be put into groups based on how they use the internet. The most important thing is that earlier works don't make any data sets available to the public so that other researchers can use them and build on them. These flaws are fixed by our work.

3. Methodology

Understanding how IoT devices use the internet is a key part of making them work better and safer. This includes being able to identify, classify, and find strange behavior in IoT devices. Several study projects have already created machine-learning-based algorithms to help with the problems of making IoT devices safer, but none of them have gone into great detail about how IoT devices' network data looks. This study collects and examines the network traffic generated by a typical smart house equipped with a range of IoT (and non-IoT) devices. Remote network servers and port numbers that the devices connect to, flow-level traffic characteristics like flow duration, and packet-level traffic characteristics like packet inter-arrival time are the three components of our study that come together to form the network traffic characteristics of IoT devices. We can use the valuable insights our study provides to improve security and speed techniques for IoT devices by understanding their behaviour and operation.

This study looks at network traffic in a typical smart home environment with 10 IoT devices and 5 non-IoT devices. It examines both IoT and non-IoT devices. We interpret IoT devices in our study using a commonly accepted definition. A specified purpose and autonomous operation without direct human control characterise an Internet of Things (IoT) device. After gathering the network traffic from every device, we investigate it in depth from three perspectives: the IoT devices' connections to remote network servers and port numbers; the flow-level traffic characteristics, such as flow duration; and the packet-level characteristics, such as packet inter-arrival time. Analysing network data from both Internet of Things (IoT) and non-IoT devices, we discovered several intriguing patterns that may aid in the development of more effective IoT security solutions, including methods for recognising, categorising, and detecting anomalous behaviour in IoT devices.

4. Iot Based Network Traffic

IoT device network flows can be found using flow features. Normally, characteristics like the number of packets in a flow, the frequency of flows, the time between packet arrivals within a flow, the size of the packet, and so on, are used to identify each device type uniquely. Classes have been put together using controlled [10], unsupervised and deep learning techniques.

Smart homes, businesses, and cities are fitting more and more IoT gadgets into their infrastructure as the Internet of Things (IoT) is heralded as the next big thing to revolutionise our civilization. But, it's possible that managers of these intelligent settings aren't even completely aware of all of their IoT resources, much alone certain that every IoT device is operating safely and secure from cybersecurity threats. Using traffic characteristics gathered at the network level, we create a strong framework in this study to handle this difficulty of classifying IoT devices. We bring four distinct contributions to the table. We start by equipping a smart environment with twenty-eight distinct Internet of Things (IoT) gadgets, including appliances, motion sensors, lights, plugs, cameras, and health monitors. For half a year, we gather and aggregate traffic traces from this infrastructure, and we make some of it publicly available for usage by the community. Using statistical features like activity cycles, port numbers, signalling patterns, and cypher suites, we then provide insights into the fundamental properties of network traffic. Third, based on unique IoT device network behaviour, we create a multi-stage machine learning based classification method and show that it can identify devices with over 99 percent accuracy. We last go over the trade-offs that must be made when implementing the categorization system in real-time in terms of cost, speed, and performance. Without the need for specialised equipment or protocols, our research opens the door for operators of smart environments to keep an eye on the existence, operation, and cyber-security of their IoT assets.

The smart environments era becoming more required in daily life. The increasing prominence of the smart environments such smart cities, homes and enterprises in the world leads to a new revolutionizing the society. The main base of these smart environments is Internet of Things (IoT). The integration of IoT to enable cyberattacks to work correctly in smart environments. The WAN interface of the TP-Link access point links to the public Internet via the university network. The Internet of Things devices make use of the LAN and WLAN interfaces. In addition to many non-IoT gadgets, our smart setting has a total of 28 distinct IoT devices from various groupings. IoT devices are Internet-connected gadgets with specialised uses, such as smoke detectors and cameras. General-purpose devices, such as computers and phones, are not part of the Internet of Things.

Cameras (Nest Dropcam, Samsung SmartCam, NetatmoWelcome, Belkin, TP-Link Day Night Cloud, Withings Smart Baby Monitor, Canary, August door bell, Ring door bell), switches and triggers (iHome, TP-Link Smart Plug, Belkin Wemo Motion Sensor, Belkin Wemo Switch), hubs (Smart Things, Amazon Echo), air quality sensors (NEST Protect smoke alarm, NetatmoWeather station, Awair air quality monitor), and electronics (Triby speaker, P Not-Internet-of-things (IoT) devices were also connected to the testbed; these included PCs, smartphones, and an Android tablet. Using the computer, the Internet of Things devices were configured according to the recommendations provided by the manufacturers of each item.

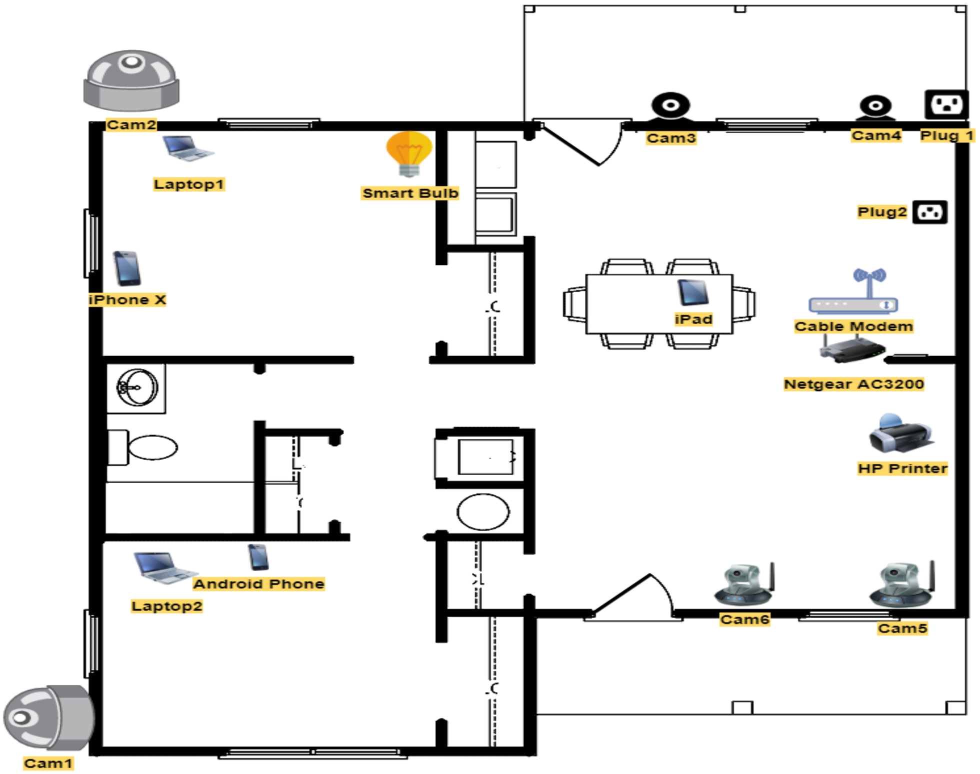


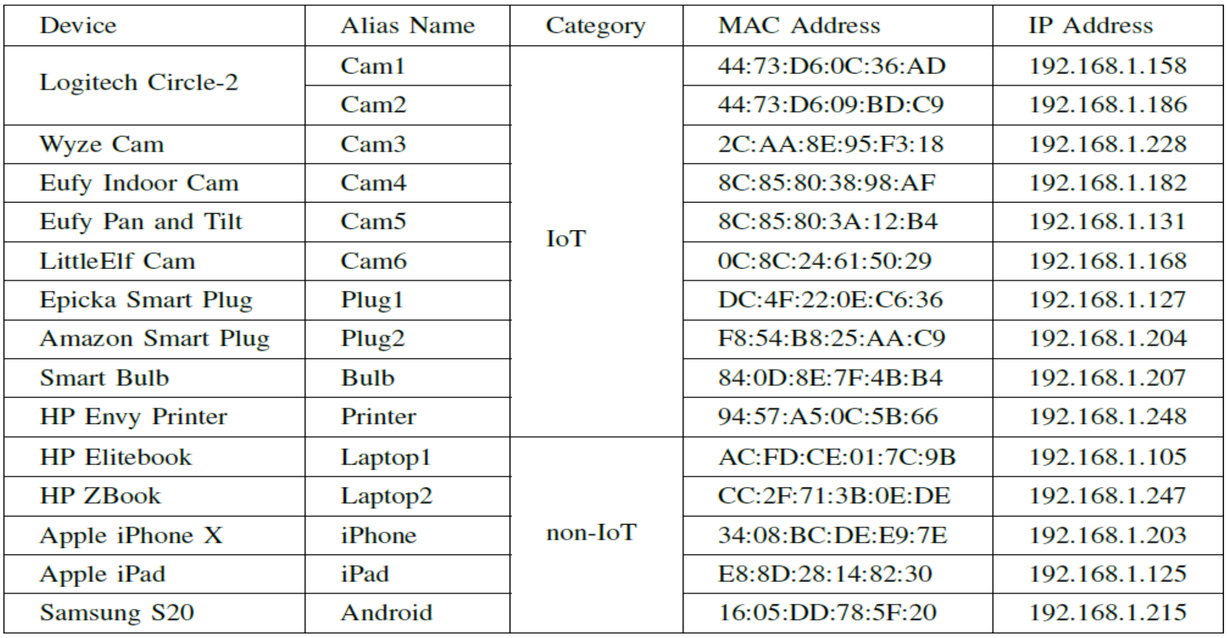
Fig 1. Smart Environment Architectural setup.

All security cams now have the ability to identify motion. When a camera detects activity, it will send video to a remote computer and send a message to the mobile app that works with it. Also, every camera has a live view feature that lets people watch live video on their phones.

To test the interoperability of IoT devices on multiple local area networks (LANs), we, for instance, connect our Android phone directly to the Technicolour router rather than the Netgear Wi-Fi router. Here are some findings we made about how different IoT devices behaved to show how different and complicated IoT device processes are. In a broad sense, different makers can make the same kind of IoT gadgets behave in very different ways. In addition, they may work differently based on where the related mobile apps are located.

5. Characerdtics Of Network Traffic

This section examines the differences between the network traffic of IoT devices and non-IoT devices based on information obtained from the home network. The features of the external computers that Internet of Things devices link to, the characteristics of the traffic at the flow level, and the characteristics of the traffic at the packet level were examined from three distinct angles. Although our data collection period spans over two months, the research will centre around the data trail we obtained on a single day which coincidentally happens to be a Monday. For some studies, we also look at the patterns of data flow on the network over the course of a week, which includes the day we talked about above. These results show how network traffic usually behaves.



Device	Alias Name	Category	MAC Address	IP Address
Logitech Circle-2	Cam1	IoT	44:73:D6:0C:36:AD	192.168.1.158
	Cam2		44:73:D6:09:BD:C9	192.168.1.186
Wyze Cam	Cam3		2C:AA:8E:95:F3:18	192.168.1.228
Eufy Indoor Cam	Cam4		8C:85:80:38:98:AF	192.168.1.182
Eufy Pan and Tilt	Cam5		8C:85:80:3A:12:B4	192.168.1.131
LittleElf Cam	Cam6		0C:8C:24:61:50:29	192.168.1.168
Epicka Smart Plug	Plug1		DC:4F:22:0E:C6:36	192.168.1.127
Amazon Smart Plug	Plug2		F8:54:B8:25:AA:C9	192.168.1.204
Smart Bulb	Bulb		84:0D:8E:7F:4B:B4	192.168.1.207
HP Envy Printer	Printer		94:57:A5:0C:5B:66	192.168.1.248
HP Elitebook	Laptop1	non-IoT	AC:FD:CE:01:7C:9B	192.168.1.105
HP ZBook	Laptop2		CC:2F:71:3B:0E:DE	192.168.1.247
Apple iPhone X	iPhone		34:08:BC:DE:E9:7E	192.168.1.203
Apple iPad	iPad		E8:8D:28:14:82:30	192.168.1.125
Samsung S20	Android		16:05:DD:78:5F:20	192.168.1.215

Table I: Smart Home Network Device Connected Devices

This section will examine the interactions that IoT devices have with external servers and the services they offer. For speed, dependability, or other reasons, it is common for an Internet of Things (IoT) device to communicate with several servers inside the same domain. Therefore, rather of organising the distant servers by individual server machines, we will arrange them by network domain. This is the reason why "remote network domain" and "remote server" refer to the same object. The associated TCP or UDP port numbers determine which external services are shown. Initially, we will examine the number of distant network domains and port numbers that a device communicates with throughout a given day. Once a week has passed, we will examine its behaviour on a daily basis. We only include the data for seven IoT devices and two non-IoT devices in the graphs to make them easier to read. Not included are the outcomes of other devices. These are comparable responses they receive.

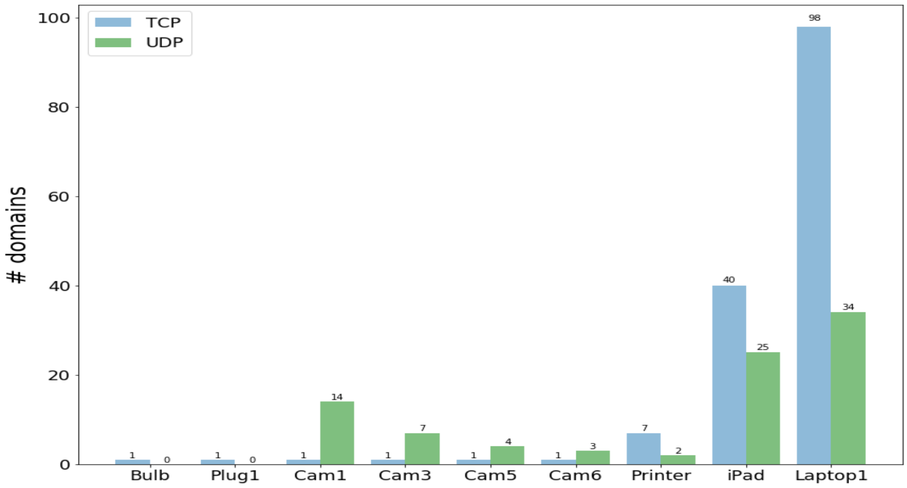


Fig 2. Various domain for remote networks in smart environment.

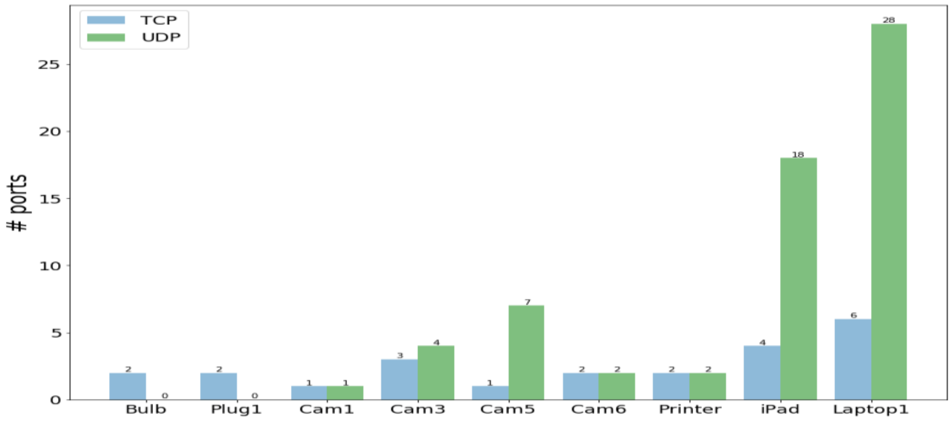


Fig 3. Various port numbers for smart environment.

Figure 2 shows how many external network domains the devices talk to on the chosen day. We offer the TCP and UDP flow statistics independently to better illustrate the device-to-device communication patterns. As the image illustrates, IoT devices are limited in their ability to communicate with external network addresses. For TCP data, the majority of IoT devices, for instance, only communicate with one network domain. For TCP, however, the Printer communicates with seven remote network domains. The Internet of Things devices often communicate with a few additional distant network addresses in order to send UDP data. In order to allow IoT devices to function independently, UDP is typically used for control data like DNS and NTP. We should point out, though, that the overall amount of UDP network addresses is actually pretty low. Non-IoT devices, on the other hand, use TCP traffic to talk to a lot more faraway network areas. Obviously, these are usually changed by how the device is used by the person who owns it. For UDP communication, non-IoT devices also have fewer distant network domains. This makes sense, since UDP is mostly used for control data like DNS, NTP, and so on. People who use these gadgets are not allowed to start any UDP traffic.

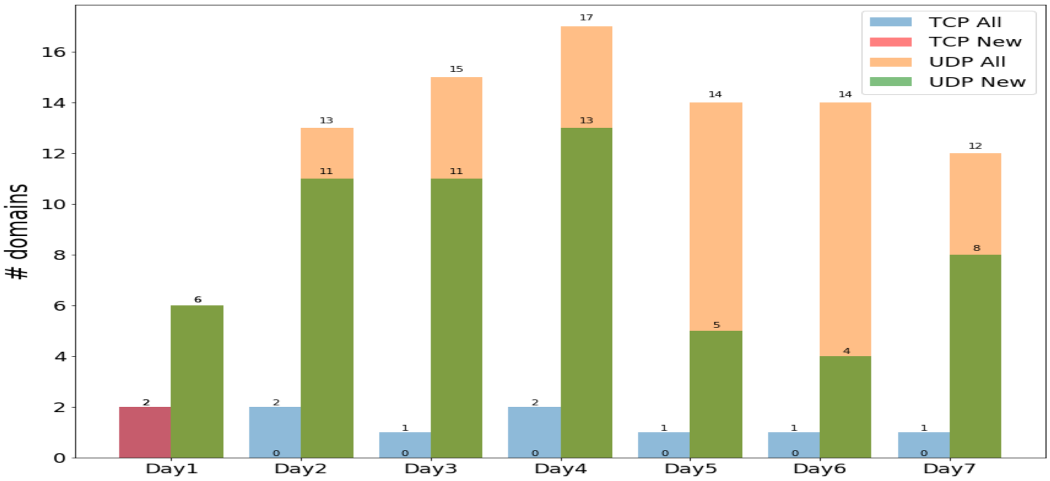


Figure 4. Various domains for smart environment with IoT devices in Cam1.

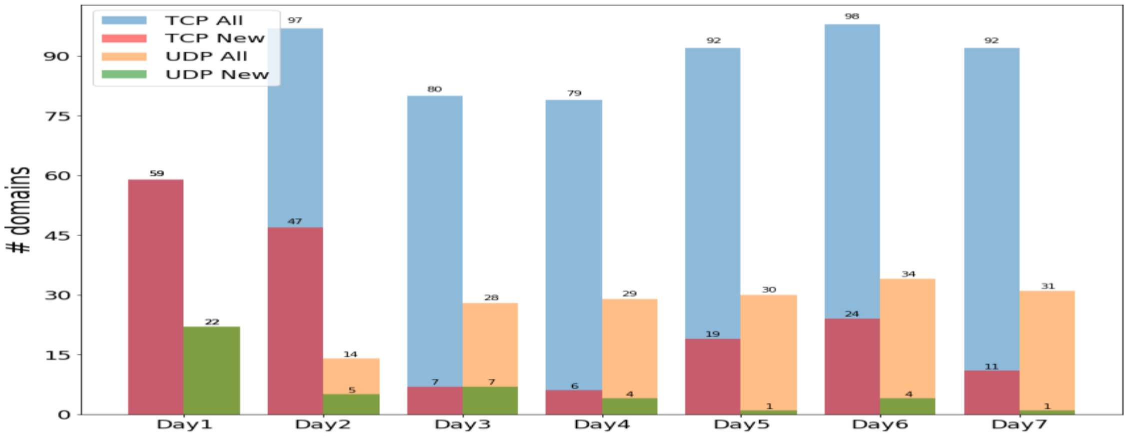


Figure 4. Various domains for smart environment with Non IoT devices in laptop1.

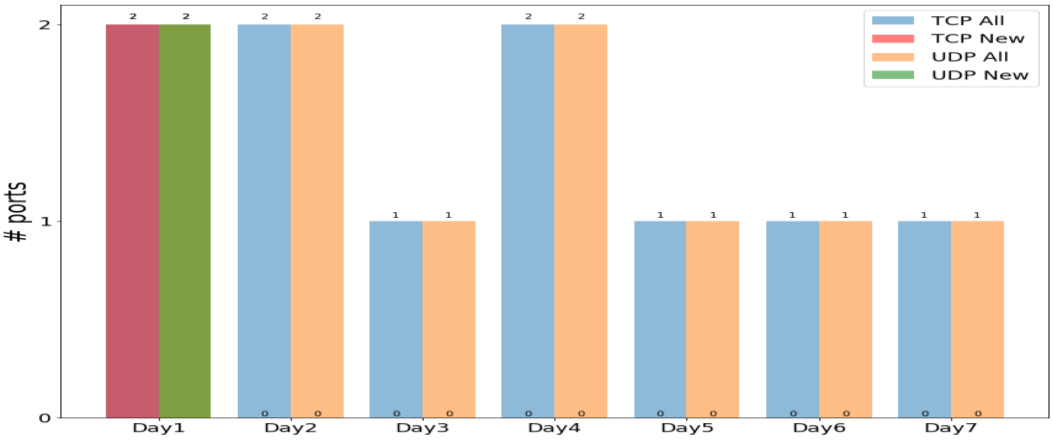


Fig 5. Various ports for smart environment with Non IoT devices in cam1.

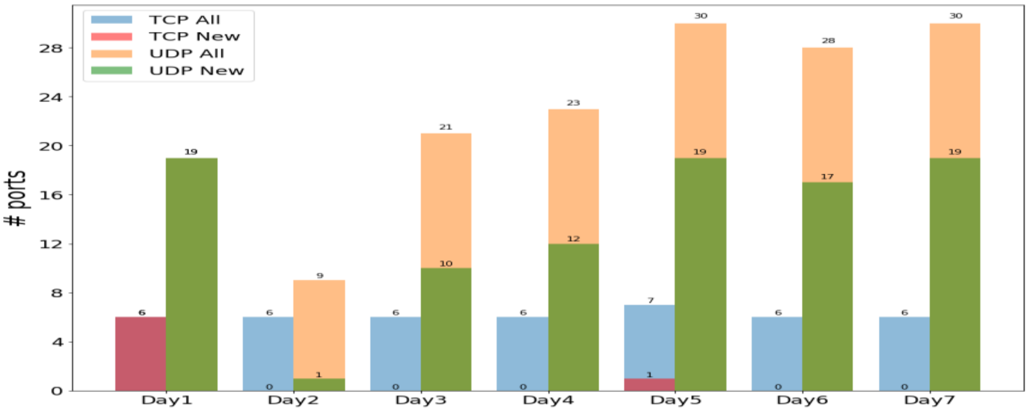


Fig 6. Various ports for smart environment with Non IoT devices in laptop1.

According to the graphic, the IoT device Cam1 only communicates with one or two external network addresses for TCP communication during the week. Amazon AWS and Cloudfront.net are the names of these services, which are a combination of Amazon AWS and a Content Delivery Network [18]. IoT devices all behave the same when TCP communication arrives. Cam1 has conversed with an increasing number of remote network domains this week, with new ones added every day, thanks to UDP activity, on the other hand. Most UDP flow is composed of DNS and NTP queries. Different from TCP communication, UDP transmission between IoT devices exhibits a few distinct behaviours. Notably, no DNS nor NTP services are communicated with by Plug1 or Bulb, the Internet of Things devices.

The way non-IoT devices act is very different from how IoT devices act. As we can see from the graph, Laptop1 talks to a lot of different external network sites using both TCP and UDP. Besides that, it talks to new faraway network domains every day. This is a good point to make, since the people who use a non-IoT device have a lot to do with how it acts. Users are able to connect to any number of websites and online applications. However, the likelihood of preprogrammed activities in IoT devices means that they are less likely to connect to haphazard external network sites and apps. Figure 3c shows how many remote port numbers Cam1 talks to every day. We can see from the picture that Cam1 only talks to a small group of stable remote port numbers. For instance, there are variations in the quantity of distant port numbers; but, beyond the initial day, no more port numbers are seen. However, as can be seen in Figure 3d, Laptop1 nearly always communicates with new distant port numbers for UDP communication (and occasionally for TCP traffic as well). This result can also be interpreted as follows: IoT devices are often pre-configured with a set of apps, which limits the number of remote ports they can communicate with to a manageable quantity.

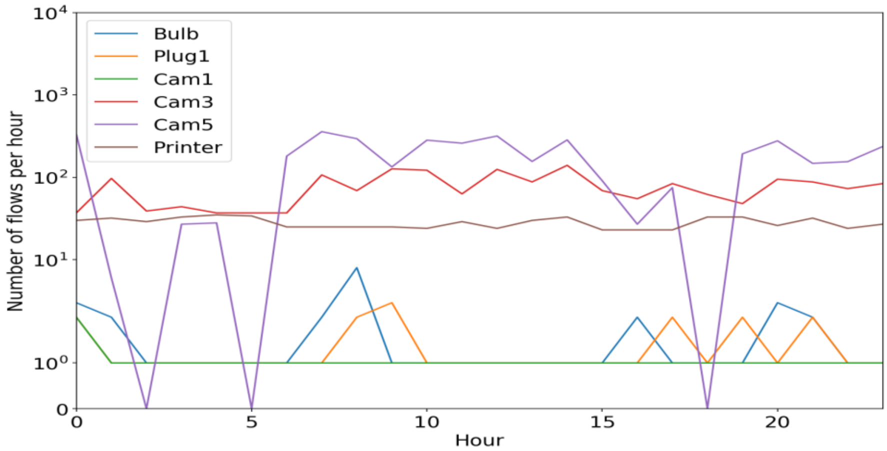


Fig 7. Various ports for smart environment with IoT devices.

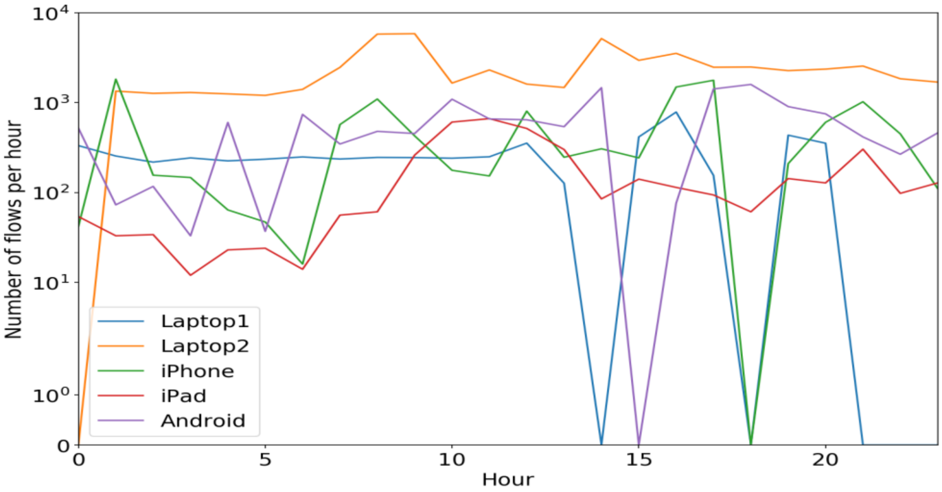


Fig 8. Various ports for smart environment with Non IoT devices.

One type of IoT traffic is traffic that devices create on their own, like DNS, NTP, and other protocols that don't need to be changed by humans. The other kind of traffic is that which users generate when they interact with devices. Examples of this include the Amazon Echo responding to voice commands, the LiFX lightbulb changing colour and intensity in response to user requests, the Belkin Wemo sensor detecting movement, and the Netatmo Welcome camera alerting the Li Our dataset is well suited to gather these two categories of IoT traffic from a lab that functions as a real-time smart environment—that is, it captures traffic both in and out of human presence.

6. Traffic Classification with Mcahine Learning

Before we can put together the traits from our trace data, we use the Joy tool [3] to turn the raw pcap files into flows every hour. Next, using the hourly samples we discussed earlier, we determine the signalling characteristics and traffic activities for a specific IoT device. Whether a device is online for an extended period of time or generates traffic through interactions with other devices determines how many instances it has for each device in the 26-week trace. There were only 13 hourly cases for the Blipcare BP monitor, for example, because it only makes traffic when someone uses it. We did, however, gather 4177 cases for Google Dropcam.

In the near future, there will be a huge number of IoT gadgets on campuses and in towns. These organisations' managers may not even be aware of all of their IoT assets, much less know if each one is secure from hackers and operating properly. Network traffic analytics, according to this study, may be used to characterise IoT devices and determine their typical behaviour. Initially, we collect and aggregate traffic data from an intelligent campus environment that has a range of Internet of Things (IoT) devices, including cameras, lighting, appliances, and health surveillance systems. We have made our three-weekly collection of data, which we call open data, available to everyone. Then, we analyse the network traces to characterise statistical characteristics of over twenty installed Internet of Things (IoT) devices, including data rates and burstiness, activity cycles, and communication patterns. Lastly, we utilise these features to develop a classification technique that is able to distinguish between data that is not connected to the Internet of Things and data that is, and we are able to identify individual connected devices with an accuracy rate over 95%. Managers of campuses and smart cities may now locate and monitor their IoT equipment by using our study's analysis of their network behaviour.

7. Results and Discussion

In the final step, we add the results from stage-0 classifiers to stage-1 without giving stage-1 any information about the quantitative attributes from stage-0. We also add quantitative attributes (flow volume, length, rate, sleep time, DNS and NTP intervals) to stage-1. Table 2's last column shows how well the classification scheme worked overall. It's very accurate in this case, with a result of 99:88% and an RRSE of only 5:06%. Almost all classes are correctly labelled.

Fig. 11 displays our complete classification's confusion matrix when all of the characteristics are applied together. With the exception of the Google Chromecast and the Hello Barbie, it verifies that all diagonal entries, which indicate proper categorization, are at or very near 100%. The Hello Barbie is sometimes referred to as a Hue lamp, while the Chromecast is occasionally referred to as the Dropcam, as was previously mentioned.

Our prediction should be much more accurate when the three categories of words—port numbers, domain names, and cypher suites—are combined, as the "Combined stage-0" column in Table 2's fourth column illustrated. 97:39% is the overall accuracy, while 18:24% is the root mean square error. Clearly, the majority of the test cases are correctly marked, with the exception of Hello Barbie. Its name, Dropcam, comes from the fact that, as we have stated previously, the most of the Hello Barbie attributes are empty in stage-0.

Though stage 0 accuracy was not very excellent, it's interesting to note that every test case of the Blipcare BP monitor has been appropriately identified. Despite the fact that the outputs of the stage-0 classifiers and the true class of the training instance are not always the same, our decision tree-based classifier in stage-1 detects a substantial correlation between the two. For instance, Ring doorbell might be the tentative result of the remote port number classifier, Dropcam could be the tentative result of the cypher suite classifier, and less than 0:66 cop could be the confidence level obtained from the domain name classifier?

In order to get the characteristics on the fly, the infrastructure needs to be able to see enough of the network information. When network switches are equipped with special hardware-accelerated flow-level analysts, like NetFlow-capable devices [37], it's not hard to get information about flows, like their volume, length, and rate. We think that the cost of extracting flow-related attributes is pretty low, and you can see them as blue bars in Fig. 12(c), which shows how the costs and benefits of the different attributes compare.

Flow-aware network switches can get information like the amount of DNS/NTP requests, the sleep time, and the bag of port numbers. They do this by doing extra math and state management. For instance, for the bag of port numbers, you need to write down the remote port numbers of all the flows that are connected to a certain IoT device. On the other hand, this particular state is not recorded by default in product switches. For the same reason, the time between each NTP/DNS UDP message should be recorded, which needs more work.

It is clear that the predictor reaches a peak level of accuracy of 96.2% after just one day of training and a plateau level of 96.6% after 16 days of training. When the training lasts 16 days instead of 1, however, the RRSE drops from 14.43% to 7.5%. The rate drops even more to 5:82% when 71% of all instances from the past 128 days are used to train. As was said in x5, the RRSE number depends on how accurate each class is. Because of this, we think that our classifier would do better in terms of RRSE if there were an equal number of cases from each class.

8. Conclusion

In the present study, we examined the behaviour of IoT device network traffic in a typical smart home environment using a collection of standard IoT (and non-IoT) devices. We examined network traffic behaviour from the perspective of IoT devices, examining features at both the flow and packet levels. Our investigation yielded valuable insights on the functionality and behaviour of IoT devices. Our ability to create faster and more secure techniques for IoT devices may be enhanced by this knowledge. Smart homes, organisations, campuses, and communities all around the world are home to a large number of Internet of Things (IoT) gadgets. Nonetheless, the administrators are unaware of what IoT devices are linked to their networks, the volume of data they are transmitting and receiving, or even whether the devices are operational and secure. This work is the first attempt to systematically classify and describe IoT devices in an operating state. Over a 26-week period, we continuously monitored traffic using a smart setup comprised of 28 distinct IoT devices. Next, we employed statistical techniques to depict the traffic in terms of activity patterns, communication protocols, cypher suites, and signal styles. With more than 96% accuracy, we have developed a machine learning-based multi-stage classification system that can recognise IoT devices. Finally, we looked at how our classification method measured up in terms of real-time operating cost, speed, and accuracy. This study demonstrates that IoT devices can be accurately identified by the way they behave on a network. It also lays the groundwork for future research that will focus on finding bad behavior in the smart environment caused by security breaches.

References

[1] 3GPP, ”Service Requirements for Machine-Type Communications,” TS 22.368 V10.1.0, June 2010.

[2] Y. Morioka, ”LTE for Mobile Consumer Devices”, ETSI Workshop on Machine to Machine Standardization, 2011.

[3] 3GPP TR 37.868 v0.8.1 (2011-08),”Study on RAN Improvements for Machine-type communications (Release 10)”.

[4] IEEE802.16p, Machine to Machine (M2M) System Requirements Document (SRD), Aug 2012.

[5] T. Taleb and A. Kunz,”Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions,” IEEE Communication Magazine, March 2012.

[6] S. Krco, J. Vuckovic, and S. Jokic, ”ecoBus Mobile Environment Monitoring”, Book Chapter in Towards a Service-Based Internet, 2010.

[7] Ravindra Changala “A Survey1 on Clustering Techniques to Improve Energy Efficient Routing in Wireless Sensor Networks” in International Journal of Applied Engineering Research ,10(58), pp.-1-5,2015.

[8] Ravindra Changala, “Secured Activity Based Authentication System” in " in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[9] Ravindra Changala, “Object Tracking in Wireless Sensor networks using Data mining Techniques”, in IOSR Journal of Electrical and Electronics Engineering, 2015.

[10] K. Moskvitch, “Securing IoT: In your Smart Home and your Connected Enterprise,” Engineering Technology, vol. 12, April 2017.

[11] N. Dhanjani, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. O’Reilly Media, 2015.

[12] E. Fernandes et al., “Security Analysis of Emerging Smart Home Applications,” in 2016 IEEE Symposium on Security and Privacy (SP). IEEE, may 2016.

[13] T. guardian. (2016) Why the internet of things is the new magic ingredient for cyber criminals.

[14] T. Yu et al., “Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things,” in Proc. ACM HotNets, Nov 2015.

[15] Sivanathan et al., “Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices,” in Proc. IEEE ANTS, Nov 2016.

[16] Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.

[17] Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.

[18] Ravindra Changala, MapReduce Framework to Improve the Efficiency of Large Scale Item Sets in IoT Using Parallel Mining of Representative Patterns in Big Data, International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 9, Issue 6, Page Number: 151-161, November 2022.

[19] R. Ferdous et al., “On the Use of SVMs to Detect Anomalies in a Stream of SIP Messages,” in Proc. IEEE ICMLA, Boca Raton, Florida, USA, Dec 2012.

[20] M. Z. Shafiq et al., “A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization,” in Proc. ACM Sigmetrics, England, Jun 2012.

[21] N. Nikaein et al., “Simple Traffic Modeling Framework for Machine Type Communication,” in Proc. ISWCS, Germany, Aug 2013.

[22] M. Jadoul. The IoT: The Network Can Make It or Break It.

[23] Ravindra Changala, A Dominant Feature Selection Method for Deep Learning Based Traffic Classification Using a Genetic Algorithm, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN : 2456-3307, Volume 8, Issue 6, November-December-2022, Page Number : 173-181.

[24] D. Bonfiglio et al., “Revealing Skype Traffic: When Randomness Plays with You,” SIGCOMM Comput. Commun. Rev., vol. 37, no. 4, pp. 37–48, Aug. 2007.

[25] Andrea et al., “Internet of Things: Security vulnerabilities and challenges,” in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015.

[26] Ravindra Changala, A Novel Approach for Network Traffic and Attacks Analysis Using Big Data in Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering: 2320-9798, Volume 10, Issue 11, November 2022.

[27] M. Iliofotou et al., “Exploiting Dynamicity in Graph-based Traffic Analysis: Techniques and Applications,” in Proc. ACM CoNEXT, Rome, Italy, Dec 2009.

[28] P. Svoboda, M. Laner, J. Fabini, M. Rupp, F. Ricciato, ”Packet Delay Measurements in Reactive IP Networks”, IEEE Instrumentation & Measurement Magazine, 2012.

[29] [29] Ravindra Changala, “Diminution of Deployment Issues in Secure Multicast System with Group Key Management” published in International Journal of Computer Application (IJCA), Impact Factor 2.52, ISSN No: 2250-1797, Volume 2, Issue 3, June 2012.

[30] M. Z. r Shafiq, L. Ji, A. X. Liu, J. Pang, J. Wang, ”A First Look at Cellular Machine-to-Machine Traffic Large Scale Measurement and Characterization”, SIGMETRICS 2012.

[31] Moore and D. Zuev, “Internet Traffic Classification Using Bayesian Analysis Techniques,” SIGMETRICS Perform. Eval. Rev., vol. 33, no. 1, pp. 50–60, Jun. 2005.