A Roadmap to Smart Homes Security Aided SDN and ML

Tanzeela Altaf and Robin Braun
School of Electrical and Data Engineering,
University of Technology Sydney, Australia
tanzeela.altaf@student.uts.edu.au.

***Abstract*—The smart home is one of those significant technology trends which enhances comfort and allows the integration of environment-friendly smart applications in daily life. It contains a large pool of internet-enabled devices some of which have a limited capability and operate in a specific manner. Due to heterogeneity and operational complexity, home networks pose extremely challenging vulnerabilities concerning privacy and security. This paper is a review of recent attempts to provide privacy and security in IoT smart homes. We summarize the research efforts in the past few years, discuss and classify them based on technologies deployed i.e. SDN, ML. We then propose an approach for the integration of SDN with ML in the home network for an automatic and reconfigurable network security mechanism. We emphasize that the proposed approach addresses the heterogeneity and scalability issues (by implementing SDN) as well as pave ways to prevent harmful attacks efficiently and in a timely manner.**

***Index Terms*—Keywords–SDN, IoT, Security, Smart homes, ML.**

I. Introduction

A smart home is one of the potential areas of IoT where users can control home devices conveniently from anywhere and at any time. By definition, a smart home refers to the ability to control, monitor, manage and provide a context-aware service to a home surrounding according to owner's will [1], [2]. A smart home network incorporates computing techniques to interact with the smart appliances, smart heating, lighting system. It also recognizes the activity of a home user [3] either by a smart sensor or a web interface. That may be voice or gesture recognition, computer vision and human behavior [4], [5]. With a smart home utility, users are able to access their homes remotely and manage it conveniently in one of several ways i.e. operate temperature sensors, control lighting system and security cameras to see if home is empty.

Thus, a smart home is a revolution where human intervention is reduced to minimum. Everyday basic tasks and internal as well as external surroundings of a home can be controlled regardless of time and distance. According to an analysis by Gartner [6], there has been a substantial year-over-year growth in the sales of smart home devices. It still has not reached to its full potential because there is a gap in consumer's demand and manufacturer's expectations. These devices are produced by different manufacturers and often these are interdependent on each other within the area of home network [7].

978-1-6654-7964-6/22/$31.00 ©2022 IEEE

IoT based Smart homes are prone to cybercrime and security exploitation which so far is a major downside of IoT as user sensitive information is carried out on the network at any time. Most of the communication between devices is unencrypted [8]. Recent attacks like Mirai show that they are also evolving with technology and becoming even more dangerous. Once a hacker gains an access, it is easy to exploit whole network via spoofing, eavesdropping or generating flood attack to achieve his purpose. It comes as no surprise in today's world that a hacker can hack into a toaster and access someone's entire network.

Smart homes consist of heterogeneous sensors with no uniformity in device's standards. Devices may be connected to each other and to the internet at all the time. Different modes of connectivity of different devices make it highly challenging with respect to communication medium and protocols. It is not possible to apply the same defence mechanisms to attacks in IoT as are applied in the conventional network [9]. There is a need to devise automated security solutions that can eliminate these evolving attacks.

To cope up with the security loopholes in smart home technology is a major research challenge that has still not met the requirements to its full. This paper entails a extensive review of literature on smart home security leveraging the services of Software Defined Networking (SDN) and Machine Learning (ML). SDN is contributing towards control and management of whole network. It minimizes the needs of firewalls and other management services for the overview of whole network. Whearas ML is one of the best ways of classifying traffic. We believe that together as an integrated vision of SDN-ML technologies there is a huge future research potential especially in the case of IoT networks where one the main issue is heterogeneous devices in one network.

Our survey represents one of the first works in the literature to systematically investigate the joint usage of SDN and ML-based security mechanisms in the complex and heterogeneous environment of IoT based smart home. This survey includes an implementation design of proposed solution using integrated approach, allowing us to highlight the objectives as well as the complementarity in manifold IoT environments. We conclude by describing the future directions in this domain.

This paper offers a systematic review of the literature on smart home security under the services of SDN and ML published in the last 5 years (2016–2021). The search was carried out on

2022 5th Conference on Cloud and Internet of Things (CIoT) | 978-1-6654-7964-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/CIOT53061.2022.9766525

3 main search engines i.e. GoogleScholar, Web of Science and IEEE explorer. After identifying a core of roughly 50 papers on the background, attacks, recent implementation strategies and network management strategies, we classified them based on several key dimensions described in the tables, and analysed a few trends within. The survey presents some of core theoretical parameters of emergent technologies in IoT based smart homes, determines that both the technologies complement each other in various ways. Our most surprising finding may be the fact that until recently, most of the literature presents SDN and ML-based security mechanisms separately in IoT despite the wealth of published material on the topic. It clear shows that this research domain requires more exploration to unleash its advantages. As a foundation, the paper layout begins by describing the background of smart homes, SDN and ML. The work narrates recent literature on related work, compares and summarizes it in tabular form and analyse the trends. At the end is conclusion and future scope of research paper.

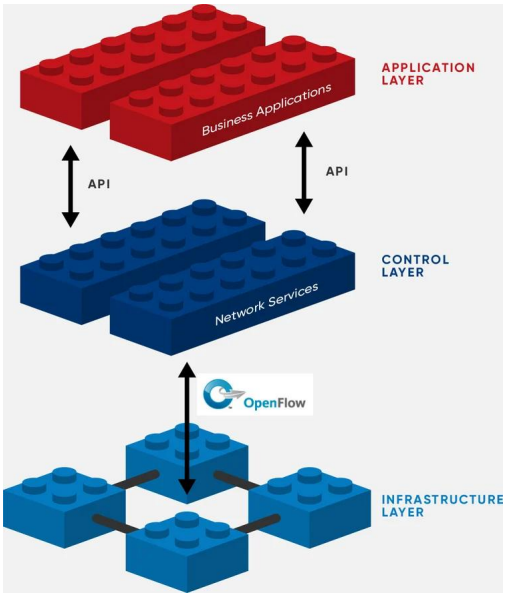

Figure 1. SDN Architecture [10]

II. Related Work

In the first section, we review and organize the research work done in the past using SDN and ML for achieving security and privacy to the IoT based smart homes.

A. Software Defined Networking

SDN has been put forward with the concept of programmable network platform through which network traffic management can be done via a software. SDN splits control plane from data plane and defines a centralised controller in the network which monitors the performance and adjusts network configuration dynamically. The controller maintains a global view of a network and provides vendor independent control over the complete network. As a result, network manager can easily change network configuration to provide smooth operation for devices, services and platforms [11]. SDN can become an integral part of IoT and there is an ongoing research worldwide for integrating SDN with IoT.

Although many research papers have broadly analyzed IoT systems and relevant security challenges we choose some of the latest works in the databases i.e. IEEEXplorer, ScienceDirect and GoogleScholar to highlight the available trends and find gaps that provide the researchers with a road map towards the proposed integrated vision.

In [12], security features of SDN/NFV are analysed, a comparison is presented on other security countermeasures with SDN/NFV based solutions. Awais et al. [13] emphasize on integration of SDN/NFV in 5G environment in order to defend the network against DDos and Authentication attacks. In [18], various challenges in smart networks are discussed and emphasizes that most of the challenges in the area of smart home, smart transportation and smart e-health can be overcome by integrating SDN in the network. An overview of IoT architecture is entailed based security and a new gateway layer is proposed for the security of IoT perception layer [14] with the implication of SDN for flexible configuration and centralised management.

Authors in [15] work on preserving privacy of IoT environments is based on the assumption that attackers rely on previously used sensitive data in an attempt to collect information on the network. Thereby, an integration of SDN, IoT and MTD is proposed and real addresses are replaced by fake addresses in order to create more complexity and ambiguity in the network for the attacker. Though it is an effective technique but it has added computational load on the network.

Any vendor specific controller can be put into practice provided that it can communicate with devices through a communication medium. The interfaces are vital for the development of SDN in assisting applications with different needs of network resources. The interfaces should be open in terms of different apps, controller and device providers. In order to attain maximum advantage from new network architecture. The controller connects with application layer through north bound interface and with underlying network devices through south bound interface. The article limits its scope to the comparison of SDN architecture, its evolution and future scope. There is no discussion about issues like availability, security and scalability in SDN [21].

Some of the remarkable advantages of incorporating SDN with IoT are: Efficient utilization of network resources, intelligent routing traffic, giving a perception of underlying resources, and simplifying the decision-making and action implementation process. Smart algorithms need to be introduced in SDN framework in order to get a maximum benefit of it [22]. In [16], SDN together with light-weight authentication protocol and OAuth framework is used to provide Authentication and Authorization before allowing the communication of IoT devices in the network. DDos attack is said to be mitigated in a timely fashion by implementing an entropy based detection algorithm at the SDN controller [23].

Table I
SDN SECURITY REVIEW

Ref.	Method used	Attack type	Validation Strategy	Performance metrics	Comparison with other studies
[12]	SDN/NFV	H/W Trojan, Replication,Tampering, Battery draining and Malicious Code injection attacks	Survey	Scalability, programmability, energy efficiency and mobility support	YES
[13]	SDN/NFV	DoS/DDoS	Review	Prompt detection and prevention	YES
[14]	SDN	Network traffic anomalies (DDoS attack mostly)	Simulations	-	NO
[15]	SDN/MTD	Identity attacks	Simulations	N/W stability, monitoring and control	NO
[16]	SDN together with protocol and framework	N/W access control	-	N/W management	YES
[17]	SDN/NFV	Dos attack	Simulations	Security and scalability	YES
[18]	SDN	User security, Data theft, traffic attacks	-	Low-level auto-reconfiguration of devices	NO
[19]	SDN	Authentication and Replay attacks	Simulation	Privacy and low computational complexity	YES
[20]	SDN	Authentication	-	Privacy and low computational complexity	YES (in computational cost)

Given below is table 1 which highlights previous study in terms of suggested methodology(ies) of security and privacy to be deployed, attacks targetted, performance metrics considered, validation strategy, and a comparison with similar studies in the literature. It is clear from the table that SDN is used against attacks due to its capability to manage and add flexibility in the network. Previous research work is mostly focused on successful attempts on integrating SDN-IoT by investigating the advantages of SDN and implying its network centric features in a way to gain maximum benefit. More performance metrics can be evaluated and improved by applying ML security algorithm.

B. Machine Learning

ML is a type of Artificial Intelligence that empowers a framework to learn from previous data rather than through explicit programming. However, ML is not a straightforward procedure. It consists of a variety of algorithms which act as building blocks to the whole system. Their job is to create a logic by learning from the training data and predict outcomes close to reality. The more training data an algorithm ingests, the more accurate the model is. Also, choosing a right algorithm is very important and can be achieved by trial-and-error in most cases. ML can be grouped into three main categories [34].

1) Supervised learning: Supervised learning is used in a case when a certain problem has an established set of data and a significant information as to how that data is classified. It tends to figure out patterns in the incoming data that can be applied to a category that define the meaning of data.

2) Unsupervised learning: Unsupervised learning is applied in a case when a problem has a massive amount of unlabeled data. This category includes a set of algorithms that can help classify this massive amount of data based on patterns or features into groups or clusters. So, it is a process to help change an unlabeled data into a labeled datat so that it becomes supervised.

3) Reinforcement learning: Reinforcement learning is a behavioral learning model and is applied to the problems where future actions are based on the output of present responses and next actions are required to be forcasted. In order to get a precise outcome, feedback is received by algorithm after analysing the data. As the system learns through trial and error, a sequence of successful decisions will result in the process being “reinforced” because it best tackles the current issue.

4) Neural networks and deep learning: A neural network consists of set of algorithms that aspires to find links in the incoming data in a much similar way as a human brain may operate. it contains three or more layers: an input layer, one or many hidden layers, and an output layer. Data is fed through the input layer and modified depending on defined weights on the nodes of hidden layer and output layers. A neural network may comprise of hundreds or even millions of nodes connected to eachother. The typical neural network may consist of thousands or even millions of simple processing nodes that are densely interconnected in one layer. The term

Table II
MACHINE LEARNING SECURITY REVIEW

References	Literature Method used	Attack type	Validation Strategy	Performance metrics	Control	Comparison with other studies
[24]	Review on Forensics and deep learning mechanisms	Bots	Survey	-	-	YES
[25]	SVM Method	Network attacks(mutation code detection)	Simulation	Accuracy	Partially centralized in terms of data storage	NO
[26]	Hidden Markov Model(HMM)	Network anomaly detection	Test bed Simulation	Accuracy	Central data storage	YES
[27]	Fusion of statistical and ML techniques	Network anomaly detection	Test bed simulations	Threshold determination for accuracy achievement	Assumes central data storage(gateway connected to sensors)	NO
[28]	Multi-stage ML algorithm	IoT device type detection	Emulation	Accuracy and Root Relative Squared Error (RRSE)	External USB attached with gateway to store data	YES
[29]	ML algorithms	Voice command fingerprinting attack	Simulations	Accuracy and Semantic distance	-	NO
[30]	Federated learning and data aggregation	Anomaly detection	-	Efficiency and better control	Cloud storage	NO
[31]	Supervised ML, ANN,KNN,	Device security and N/w security	Survey	-	-	NO
[32]	ML algorithms and DL	Authentication, Dos, IDS, Malware	Survey	-	Distributed	YES
[33]	DELM and Block Chain	Intrusion detection	Simulations	Accuracy, Miss Rate, Sensitivity, Specificity, False Positive Value, and Positive Prediction Value	Decentralized	YES

deep learning is implied when a neural network consists of more than one hidden layers.

Several studies in the literature have attempted to employ ML to design a security and privacy mechanism for IoT based smart homes. We chose the latest papers to road map the gaps and trends in case of ML based smart home security.

In an survey, Koroniotis et al. [24] suggested to deploy deep learning and forensics techniques in the IoT architecture in order to expose botnets. Furthermore, applicability of network forensics is investigated and challenges are highlighted. Hou et al. [25] has built an SVM based classifier in an effort to provide a clear difference between mutation and regular codes in order to detect network attacks particularly in a smart home environment. The network detection system offers less complexity and behaves in a timely manner by dividing the incoming data into one of two categories and paves ways towards finding network attack information. In another approach [26], real-time data is generated from a testbed consisting of multiple sensors deployed in a smart home environment i.e. smart plugs, google assistant, wireless sensor tags and NestProtect. Then, the data is trained through a hidden Markov Model (HMM) of ML and abnormal behaviour is detected with 97% of accuracy by the HMM behavioural modelling of sensors. However, the work considers limited and specific devices and does not take in account the presence of more than one resident. A similar solution is proposed in [27], where behavioural device templates are constructed by the fusion of statistical and ML techniques with respect to smart home network behaviour. Anomaly is detected based on the idea that compromised device will move away from the centre of cluster which is developed after the statistical metrics are gathered. More work needs to be done in order to get an optimal threshold and threat score which ultimately defines the performance of this system.

In an effort [28] to identify the behaviour of smart devices with in smart environment, ML based framework is explored (with the help of network traffic characteristics). The work does not deal with security of devices directly but can be made

a foundation towards achieving security from the behavioural modelling of devices. This work [29], targets the security and privacy of smart home speakers in particular. Privacy leakage is investigated and voice command fingerprinting attack is focused which is essentially a type of traffic analysis. Whereas more work needs to be done on this side. In [30], IOTFLA architecture is proposed based on the idea of federated learning in IoT based smart homes to cater data security and privacy. It's merits and demerits are discussed in terms of implementation in the world of IoT. In [33], authors present resource efficient ML and block chain based security solution to smart home network.

Table 2 is a synoptic view of the previous work in terms of suggested methodology(ies), targeted attacks, performance metrics, validation strategy, and a comparison with similar studies in the literature. The practical realization of most of ML based schemes is not hindered by technical issues, but by the lack of availability of training data and resources for efficiently accessing and analysing ongoing network traffic features that can in turn abstract from detecting attacks in a timely manner. It emerges from the table that a variety of performance metrics can be evaluated using ML algorithms due to its ability to classify traffic effectively. We can enhance capability of an ML model by adding SDN and giving a network centric global view to ML model.

C. SDN and ML integration

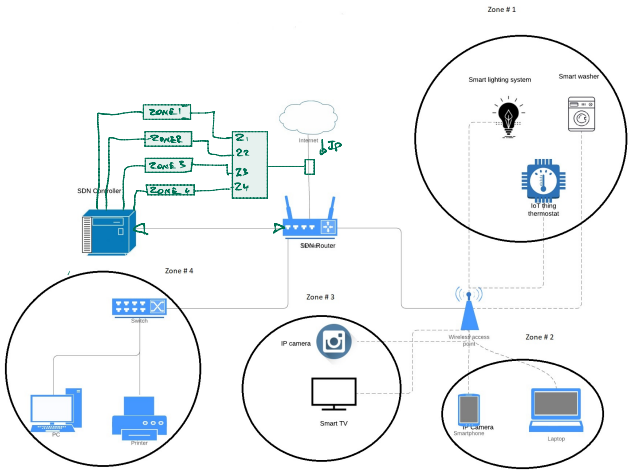

Figure 2. Smart home architecture

This section enlists nearly all the research papers from the past that have worked on the integrated vision of SDN and ML for achieving security or privacy in IoT applications. This section is an update to all the past work done on security and privacy using SDN-ML approach. We come to the conclusion that when considering this approach in IoT environments very little work done in the past. [35] is a good attempt to provide a roadmap of open research challenges when applying SDN/ML concepts and thus is a step forward towards IoT security. Tang et al. in [36] and [37] has used deep learning for SD-IoT environment to predict future network traffic loads at switches and further assign channel resouce. This is not related to security of IoT but advocates to traffic congestion in SD-IoT environment which can be modelled towards achieving security in IoT. [38] explores ML methodologies with the aim of anomaly detection SD-IoT network environment. Similar work is proposed in [39] where ML is leveraged to enhance security of SDN based IoT architecture. A lot of work has been done in catering that security loopholes of SDN with the help of ML whereas this is out of scope of this paper since we are reviewing the security of IoT architecture in context of SDN- and ML- integration. We come to the conclusion that there is no such work presented specifically in a smart home environment.

Table 3 presents previous study in terms of inclusion of SDN/ML review, validation strategy, objective for SDN/ML integration and which IoT application has been targetted in those papers. The table summarizes that there is no SDN/ML integration survey presented before our work in the case of smart home application of IoT. Where one such survey is done for smart cities with similar emphasis and approach, we believe that it will be very effective for smart homes specifically due to its heterogeneous and complex nature. In this way, it is the first work of its type.

In addition, it emerges that there is a need to devise a security system which can not only address heterogeneity and scalability of devices with in the home network but also access, track, and analyse the huge amounts of information being generated by different devices over time. SDN deployment can facilitate heterogeneity and scalability issue and give a centralised control over the network. SDN makes the whole network more flexible in order to add ML based network defense mechanisms.

Since our literature review displays that the research in this area is still in its embryonic stage, we aim to lay foundation for the expansion of smart home security for next generation of IoT. We believe that another key contribution of this review is represented by a detailed discussion on future research directions towards the broad deployment of SDN/ML-based security solutions in IoT.

III. Proposed Approach and Methodology

In order to test the hypothesis, following is the design model.

The design model 2 consists of a smart home network in which smart appliances are communicating with each other and to the internet. The home network is integrated with Software-Defined controller and switch in such a way that all the network traffic is passing through the switch. The controller is communicating with SD switch. For simplicity, it is assumed that home router is SDN enabled. To enable security to the whole network, it is first divided in to four set of classes based on types of devices and traffic generated.

Class A: consists of all the simple devices or sensors who can perform only a specific task. i.e Coffee machine, light bulb, smart washer.

Table III
SDN AND ML FOR IOT SECURITY

References	SDN security review	ML security review	Validation Strategy	Objective	Year	IoT application presumed
[35]	Yes	Yes	Review	Road map of challenges related to the application of ML and SDN in IoT security	2018	-
[36]	No	No	Simulations	Assigning a suitable channel to SDN-IoT switch with a purpose of avoiding network congestion	2018	-
[37]	No	No	Simulations	Forecasting traffic load and network congestion and then allocating channels to SDN-IoT	2018	-
[38]	No	No	Simulations	Exploring the use of ML for anomaly detection in IoT networks connected through SDN	2019	-
[39]	Yes	Yes	Survey	Enhancing the security of SDN based architecture of IoT	2018	Smart city
[40]	SDN	No	Simulations	Enhhancing device classification and malicious traffic detection	2021	Smart home

Class B: consists of set of smart devices that offer a wide range of capabilities, services and applications to the users i.e. smart phone, laptop, tablets.

Class C: consists of video streaming devices. i.e Security cameras, TV.

Class D: consists of wired network devices. i.e computer, printer.

Having divided the whole network in to classes, ML network defense algorithms can be designed with suitability to the traffic generated.

Here are the steps of methods with which network security is achieved: Firstly, devices that belong to different classes need an authentication before communicating with each other. This is achieved by defining a criteria against matching rules in SDN switch. Secondly, use ML based approach to train a data model and look out for intrusion, if any, in the home system. In case of intrusion, ML algorithm will feed its output to SDN controller which will then let the switch know to block that particular traffic and prevent from getting into the network

IV. CONCLUSIONS

IoT based Smart home is one of those significant technology trends which enhances comfort and allows integration of environment friendly smart applications in daily human life. It contains a vast pool of internet enabled devices some of which have a limited capability and operate in a specific manner only. In this paper, we have provided a novel prospective on one of biggest research challenge nowadays which is IoT based smart home security. This consists of a rare blend of SDN and ML based concepts. The basic idea behind this is to provide a platform through which overall architecture can be simplified and network traffic management can be done via software.

It is highly likely that with the growth of IoT services, new threats and security risks will also emerge. There is no guaranteed solution which can address all these issues at once. More work needs to be done in this direction. By deploying SDN in the architecture, network security engineers are able to monitor network behaviour, program and control it. Moreover, it provides more flexibility to add defense techniques i.e. ML algorithms in the network.

We have shed light on the services of smart home and the future research scope. Moreover, we summarized recent proposed solutions, attacks targeted and accordant state-of-art research. We argue that the risks and vulnerabilities are likely to increase with the advancement of smart home technology. Therefore, emphasis remains on the integration of SDN with IoT and the concept of ML in such a way that ongoing traffic pattern is analysed repeatedly, malicious behaviour, if any, is detected, necessary measures are taken to undo the attack and finally, suspicious link is blocked. We advocate that our network-centric notion can pave ways for security in the outgrowing smart-homes.

REFERENCES

[1] Weixian Li, Thillainathan Logenthiran, Van Tung Phan, and Wai Lok Woo. Implemented IoT-based self-learning home management system (SHMS) for Singapore. *IEEE Internet of Things Journal*, 5(3):2212–2219, 2018. ISSN: 23274662. DOI: 10.1109/JIOT.2018.2828144.

[2] Tiankai Liang, Bi Zeng, Jianqi Liu, Linfeng Ye, and Caifeng Zou. An unsupervised user behavior prediction algorithm based on machine learning and neural network for smart home. *IEEE Access*, 6:49237–49247, 2018. ISSN: 21693536. DOI: 10.1109/ACCESS.2018.2868984.

[3] Homay Danaei Mehr. Human Activity Recognition in Smart Home With Deep Learning Approach. *2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*:149–153.

[4] Farzeem D. Jivani, Manohar Malvankar, and Radha Shankarmani. A Voice Controlled Smart Home Solution with a Centralized Management Framework Implemented Using AI and NLP. *Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018*:1–5, 2018. DOI: 10.1109/ICCTCT.2018.8550972.

[5] Suraj, Ish Kool, Dharmendra Kumar, and Shovan Barma. Visual Machine Intelligence for Home Automation. *Proceedings - 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages, IoT-SIU 2018*:1–6, 2018. DOI: 10.1109/IoT-SIU.2018.8519915.

[6] Fernando Elizalde. Hype Cycle for the Connected Home , 2018. Technical report 30 July, Gartner, 2018.

[7] J. H. Sharma, P. K.; Park, J. H.; Jeong, Y.-S. & Park. SHSec: SDN based secure smart home network architecture for Internet of Things. *Mobile Networks and Applications*, 24(3):913–924, 2019. ISSN: 1572-8153. DOI: 10.1007/s11036-018-1147-3. URL: https://doi.org/10.1007/s11036-018-1147-3.

[8] Martin Serror, Martin Henze, Sacha Hack, Marko Schuba, and Klaus Wehrle. Towards in-network security for smart homes. *ACM International Conference Proceeding Series*, 2018. DOI: 10.1145/3230833.3232802.

[9] Elisa Bertino. Internet of Things (IoT): Smart and Secure Service Delivery. *ACM Transactions on Internet Technology*, 16(4):1–8, 2016. ISSN: 15335399. DOI: 10.1145/3013520.

[10] Sdx Central. Understanding the SDN Architecture, SDN Control Plane and SDN Data Plane. URL: https://www.sdxcentral.com/networking/sdn/definitions/inside-sdn-architecture/.

[11] Nachikethas A. Jagadeesan and Bhaskar Krishnamachari. Software-defined networking paradigms in wireless networks: A survey. *ACM Computing Surveys*, 47(2), 2014. ISSN: 15577341. DOI: 10.1145/2655690.

[12] Ivan Farris, Tarik Taleb, Yacine Khettab, and Jaeseung Song. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys and Tutorials*, 21(1):812–837, 2019. ISSN: 1553877X. DOI: 10.1109/COMST.2018.2862350.

[13] M. Awais Javed and Sohaib Khan Niazi. 5G security artifacts (DoS / DDoS and Authentication). *2019 International Conference on Communication Technologies, ComTech 2019*, (ComTech):127–133, 2019. DOI: 10.1109/COMTECH.2019.8737800.

[14] Shiji Zheng. Research on SDN-based IoT Security Architecture Model. (Itaic):575–579, 2019. DOI: 10.1109/itaic.2019.8785456.

[15] Abdulrahman Almohaimeed, Srikanth Gampa, and Gurtaj Singh. Privacy-Preserving IoT Devices. *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*:1–5, 2019. DOI: 10.1109/lisat.2019.8817349.

[16] Kallol Krishna Karmakar, Vijay Varadharajan, Surya Nepal, and Uday Tupakula. SDN enabled secure IoT architecture. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019*:581–585, 2019.

[17] Ozgur Akan, Paolo Bellavista, Geoffrey Coulson, Falko Dressler, Domenico Ferrari, Hisashi Kobayashi, Sergio Palazzo, Xuemin Sherman Shen, Mircea Stan, Jia Xiaohua, and Albert Y Zomaya. *Ubiquitous Communications and Network Computing*. 2017, pages 189–195. ISBN: 9783319734224. URL: http://www.springer.com/series/8197.

[18] Priyanka Prabakaran, Deva Priya Isravel, and Salaja Silas. A Review of SDN-Based Next Generation Smart Networks. *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*:80–85, 2019. DOI: 10.1109/iccct2.2019.8824871.

[19] Sdn enabled Smart Homes, Waseem Iqbal, Haider Abbas, Pan Deng, and Jiafu Wan. ALAM : Anonymous Lightweight Authentication. 8(12):9622–9633, 2021.

[20] Waseem Iqbal, Haider Abbas, Bilal Rauf, Yawar Abbas, Faisal Amjad, and Ahmed Hemani. PCSS: Privacy Preserving Communication Scheme for SDN Enabled Smart Homes. *IEEE Sensors Journal*, (c):1–13, 2021. ISSN: 15581748. DOI: 10.1109/JSEN.2021.3087779.

[21] Doan B Hoang and Minh Pham. On software-defined networking and the design of sdn controllers, Conference Paper, 2015.

[22] Keshav Sood, Shui Yu, and Yong Xiang. Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review. *IEEE Internet of Things Journal*, 3(4):453–463, 2016. ISSN: 23274662. DOI: 10.1109/JIOT.2015.2480421.

[23] Narmadha Sambandam, Mourad Hussein, Noor Siddiqi, and Chung-Horng Lung. Network security for IoT using SDN: Timely DDoS detection. In *IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2018. ISBN: 9781538615621. DOI: 10.1109/IRI.2017.44.

[24] Nickolaos Koroniotis, Nour Moustafa, and Elena Sitnikova. Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions. *IEEE Access*, 7:61764–61785, 2019. ISSN: 21693536. DOI: 10.1109/ACCESS.2019.2916717.

[25] Size Hou and Xin Huang. Use of Machine Learning in Detecting Network Security of Edge Computing System. *2019 4th IEEE International Conference on Big Data Analytics, ICBDA 2019*:252–256, 2019. DOI: 10.1109/ICBDA.2019.8713237.

[26] Sowmya Ramapatruni, Sandeep Nair Narayanan, Sudip Mittal, Anupam Joshi, and Karuna Joshi. Anomaly

Detection Models for Smart Home Security. *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*:19–24, 2019. DOI: 10.1109/bigdatasecurity-hpsc-ids.2019.00015.

[27] Georgios Spanos, Konstantinos M. Giannoutakis, Konstantinos Votis, and Dimitrios Tzovaras. Combining Statistical and Machine Learning Techniques in IoT Anomaly Detection for Smart Homes. *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*:1–6, 2019. ISSN: 23784873. DOI: 10.1109/camad.2019.8858490.

[28] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing*, 18(8):1745–1759, 2019. ISSN: 15580660. DOI: 10.1109/TMC.2018.2866249.

[29] Sean Kennedy, Haipeng Li, Chenggang Wang, Hao Liu, Boyang Wang, and Wenhai Sun. I Can Hear Your Alexa: Voice Command Fingerprinting on Smart Home Speakers. *2019 IEEE Conference on Communications and Network Security (CNS)*:232–240, 2019. DOI: 10.1109/cns.2019.8802686.

[30] Ulrich Matchi Aivodji, Sebastien Gambs, and Alexandre Martin. IOTFLA : A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning:175–180, 2019. DOI: 10.1109/spw.2019.00041.

[31] Laizhong Cui, Shu Yang, Fei Chen, Zhong Ming, Nan Lu, and Jing Qin. A survey on application of machine learning for Internet of Things. *International Journal of Machine Learning and Cybernetics*, 9(8):1399–1417, 2018. ISSN: 1868808X. DOI: 10.1007/s13042-018-0834-5. URL: http://dx.doi.org/10.1007/s13042-018-0834-5.

[32] Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. Machine Learning in IoT Security: Current Solutions and Future Challenges:1–23, 2019. arXiv: 1904.05735. URL: http://arxiv.org/abs/1904.05735.

[33] Muhammad Adnan Khan, Sagheer Abbas, Abdur Rehman, Yousaf Saeed, Asim Zeb, M. Irfan Uddin, Nidal Nasser, and Asmaa Ali. A Machine Learning Approach for Blockchain-Based Smart Home Networks Security. *IEEE Network*, 35(3):223–229, 2021. ISSN: 1558156X. DOI: 10.1109/MNET.011.2000514.

[34] Pat Langley and Jaime G. Carbonell. *Approaches to machine learning*, volume 35 of number 5. 1984, pages 306–316. ISBN: 9781119454953. DOI: 10.1002/asi.4630350509.

[35] Francesco Restuccia, Salvatore D'Oro, and Tommaso Melodia. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet of Things Journal*, 5(6):4829–4842, 2018. ISSN: 23274662. DOI: 10.1109/JIOT.2018.2846040. arXiv: 1803.05022.

[36] Fengxiao Tang, Bomin Mao, Zubair Md Fadlullah, and Nei Kato. On a Novel Deep-Learning-Based Intelligent Partially Overlapping Channel Assignment in SDN-IoT. *IEEE Communications Magazine*, 56(9):80–86, 2018. ISSN: 15581896. DOI: 10.1109/MCOM.2018.1701227.

[37] Fengxiao Tang, Zubair Md Fadlullah, Bomin Mao, and Nei Kato. An Intelligent Traffic Load Prediction-Based Adaptive Channel Assignment Algorithm in SDN-IoT: A Deep Learning Approach. *IEEE Internet of Things Journal*, 5(6):5141–5154, 2018. ISSN: 23274662. DOI: 10.1109/JIOT.2018.2838574.

[38] Perekebode Amangele, Martin J. Reed, Mays Al-Naday, Nikolaos Thomos, and Mateusz Nowak. Hierarchical Machine Learning for IoT Anomaly Detection in SDN. *2019 International Conference on Information Technologies (InfoTech)*, (September):1–4, 2019. DOI: 10.1109/infotech.2019.8860878.

[39] Ahmed Dawoud, Seyed Shahristani, and Chun Raun. Deep learning and software-defined networks: Towards secure IoT architecture. *Internet of Things*, 3-4:82–89, 2018. ISSN: 25426605. DOI: 10.1016/j.iot.2018.09.003. URL: https://doi.org/10.1016/j.iot.2018.09.003.

[40] Holden Gordon, Conrad Park, Bhagyashri Tushir, Yuhong Liu, and Behnam Dezfouli. An Efficient SDN Architecture for Smart Home Security Accelerated by FPGA. *IEEE Workshop on Local and Metropolitan Area Networks*, 2021-July:1–3, 2021. ISSN: 19440375. DOI: 10.1109/LANMAN52105.2021.9478836. arXiv: 2106.11390.

.