IoT Federated Learning Architecture: A secured and privacy-preserving smart home

ONYEWUZOR CHIOMA THERESA

onyewuzor.chioma@gmail.com

Computer Science Department, Federal Polytechnic Oko.

ABSTRACT:

Slowly but steadily, the Internet of Things (IoT) is becoming more and more ubiquitous in our daily life. However, it also brings important security and privacy challenges along with it, especially in a sensitive context such as the smart home. In this position paper, we propose a novel architecture for smart home, called **IOTFLA**, focusing on the security and privacy aspects, which combines federated learning with secure data aggregation. We hope that our proposition will provide a step forward towards achieving more security and privacy in smart homes.

KEYWORDS: Security, Privacy, Machine Learning, Federated Learning, Secure Data

INTRODUCTION

Although there is no general consensus on how to define the *Internet of Things* (IoT), in this paper we adopt the definition given by Kevin Ashton [1], which describes the IoT as a wide ecosystem in which interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. While the production of smart devices keeps increasing for a wide variety of usage and fields, for individuals this development of smart devices is also a major concern for their security as well as their privacy. This is especially the case in domains in which the data sensed and collected by the devices are personal and thus highly sensitive (*e.g.*, health, sport or smart home).

In addition, the concept of *Privacy-by-design*, which requires to take into account privacy issues as soon as the conception phase of a system rather than to wait for its deployment, has now become a legal requirement in the new European *General Data Protection Regulation* (GDPR) [2]. More precisely, Article 23 of the GDPR asks data controllers to hold and process only the data absolutely necessary for the completion of its duties as well as to limit the access to personal data to those that only requires it for the completion of a particular objective. Thus, to reach the full potential of IoT requires to be able to also solve the privacy issues raised by the development of these devices.

To address these concerns, we propose IOTFLA, an architecture focusing primarily on data security and privacy. More precisely, IOTFLA aims at enhancing the security and privacy in the IoT context by promoting the federated learning approach, which enables to train models locally, combined with the use of secure data aggregation.

Centralized model with training data distributed over a large number of clients, each with possibly unreliable and relatively slow network connections. Originally, the federated learning approach has mainly been used in the context of smartphone to improve text prediction models. First, the smartphone of a user downloads a common generic model, who is then improved locally over time with data collected and processed directly in the smartphone. From time to time, the improved local model is sent to the cloud and merged with all other user's models through secure aggregation. This update of the common generic model is then dispatched as a new update.

Nonetheless, several papers have already proposed to apply the federated learning approach in the context of IoT. For instance in [4], the authors have used the federated learning approach to suggest two strategies to improve communication efficiency by reducing the up-link communication cost, in the context of mobile phones as clients, in which communication efficiency is of the utmost importance. More recently, in [3] the authors propose an algorithm for client-sided differential privacy-preserving federated optimization to deal with differential attacks. Their main objective is to hide the clients' contributions during training while balancing the trade-off between privacy loss and model performance.

FL offers strong benefits for data privacy in general due to the local processing of personal information. However, to the best of our knowledge, no contribution in the form of architecture for smart home promoting security and data privacy using federated learning and secure data aggregation has been proposed so far. In this paper, we propose to use the context of smart home as the use case for FL, by keeping as much as possible of the data on IoT devices and by ensuring that only updates made to the models are transferred in order to allow the update of the global model.

Outline. The outline of the paper is a follows. First, in Section II, we review the background notions necessary to the comprehension of our architecture. Then in Section III, we describe the main components of our architecture as well as the main security and privacy strategies. Afterwards, we discuss how to integrate federated learning and data aggregation to IOTFLA in three different implementation scenarios. Finally, we discuss the issues related to the implementation of our architecture in Section IV before concluding in Section V.

BACKGROUND

In this section, we describe first the main architectures that have been proposed for the IoT before highlighting the main security and privacy challenges raised by this context. Afterwards, we review the existing secure data aggregation protocols.

A. Architectures for the Internet of Things

The evolution of the IoT is characterized by its ability to scale globally. For instance, according to Gartner [5], it has involved approximately 8.5 billion smart devices or things in 2017, which is 31% more than 2016 and by 2020 the number of connected devices is envisioned to reach 20 billions. With that increase, the landscape of IoT keeps changing and expanding. Several architectures have already been developed for IoT, which are usually derived from the classical three layers architecture [6] :

- *Perception layer*. This layer is made of nodes who sense, gather, collect and transmit data. Furthermore, this layer is in charge of converting the sensed data to digital signals, which is more convenient for network transmission. In the context of smart home, the components of the perception layer's are basically smart devices (*e.g.*, sensors, lights, hubs, thermostats, ...) who rely on technologies such as RFID, WSN, GPS and NFC.

- *Network layer*. This layer is in charge of processing data coming from the perception layer and also to transmit the processed data to the application layer through network technologies and protocols (*e.g.*, WIFI, Bluetooth, BLE, CoAP, RPL, MQTT, ...).
- *Application layer*. This layer uses the processed data by the network layer and constitutes the front end of the whole IoT architecture through which several applications can be developed for domains such as smart home, sports, health, business, transport and logistics.

For instance, this architecture inspired [7], in which the authors proposed a five layers architecture based on the Internet architecture and the logical structure of telecommunications management combined with the specific features of the IoT. By adding two layers, the architecture has for main objective to better explain the different features and specificities of the IoT than the generic IoT architecture.

In addition in [8], in which the authors focus on identifying the future applications and key challenges associated with the development of IoT, such as naming and identity management, interoperability and standardization as well as information privacy. In their approach, it is suggested that the structure of IoT is divided also into five layers with the addition of a middleware layer and a business layer on top of the classical three layers architecture.

Furthermore, some security enhanced architectures have been proposed. For instance in [9], the authors propose a novel security architecture for the IoT that intend to solve the relationship between heterogeneous entities and different security issues. In [10], the authors analyze the infrastructure and security risks of the IoT, which allow them to propose a new multilayer security model aiming at achieving a highlevel of privacy protection by relying on two middlewares implemented between three layers of the generic IoT architecture, in which both middleware use encryption and decryption mechanism as well as access control mechanisms.

B. Security and privacy challenges

Security and privacy are two important aspects in the context of IoT, especially in smart homes. Indeed, the IoT presents new and unique security challenges as highlighted in different papers [11], [12], [13], such as:

- *Limited resources*. The majority of smart devices have limited capabilities, in particular with respect to processing, memory and power. Thus, applying conventional security mechanisms require some modifications due to this constraint. In addition, advanced security mechanisms may not even be directly applied in this context.
- *Security integration and updates*. With respect to authentication solutions, there is no standard currently being deployed at large-scale in IoT systems. Thus, one key challenge is to be able to integrate the different security mechanisms and to make them interoperable. In addition, applying security updates is a challenging issue for IoT due to the difficulty of allowing traditional update mechanisms.
- *Insecure programming*. The IoT products market is subject to high pressure, which usually means that aspects such as functionality and usability are usually considered more important than security and privacy.
- *Wide area of attack and heterogeneous ecosystem*. The threat landscape of IoT is extremely wide due to the heterogeneity of devices and the increasing number of threats and risks and their rapid evolution rapidly and their important impact on humans safety, health and privacy. As a consequence, the creation of the security policy also requires an overview of every part of the ecosystem to apply suitable security and privacy mechanisms.

- *Snowball effect*. The interconnected nature of smart devices means that any insecure device connected to a private network (*e.g.* a smart home network) can potentially lead to the exploitation of vulnerabilities of other devices or even endanger the security of the entire system.

Meeting these security challenges has become one of the most important targets for IoT manufacturers as well as the scientific community. In addition to these security challenges, the privacy is also a major concern in a smart home context, in which the collected data is about individuals. The main privacy challenges are the following:

- *Data confidentiality*. In IoT, confidentiality is an important privacy challenge because of the heterogeneity of the devices. In particular, devices with limited computational resources may not be able to use state-of-art encryption algorithms.
- *Data anonymization*. Traditional anonymization mechanisms that aim at separating the connection between an information captured by an IoT device and its corresponding data subject are difficult to implement in the IoT setting.
- *Control on the access to the data collected*. In the IoT setting, just as in any distributed system, strong access control mechanisms are necessary to prevent unauthorized entities from gaining access to the data and to ensure that only authorized entities can only access to this data.
- *Data erasure*. All the data collected about the individuals by the objects may be retained indefinitely (at the cost of storage capacities) on the devices themselves.

C. Secure data aggregation

The last building block of our architecture is the use of secure data aggregation protocol, which is a process occurring between the *data gathering phase* (perception layer) and the *data analysis phase* (network or application layer). There are many possible implementations of this primitive, some of which have already been used within the context of the IoT. For instance [12], [13], the authors have surveyed existing protocols classified them according to criteria such as confidentiality, integrity, authentication and freshness.

In our context, confidentiality and integrity are the most important criteria that we want to achieve. In addition, we need to ensure that the chosen protocol chosen fits the architecture that we propose. Thus we have to take into account others parameters, such as the type of aggregation, the energy consumption, the network consumption, the network capabilities as well as the resources available (*i.e.*, with respect to network and devices). Focusing at first solely on the confidentiality and integrity criteria reduces the number of appropriate secure aggregation protocols to the following ones:

- SecureDAV [14] is a cluster-based aggregation protocol in which the network is divided into groups, which also uses Merkle hash-trees construction. It relies on ellipticcurve cryptography, which enables to use small size keys leading also to faster computation and the reduction of energy consumption.
- ECIPAP [15] is an efficient aggregation protocol ensuring the confidentiality and integrity of data. It is composed of three different phases: (1) query dissemination, (2) aggregation of data and (3) verification of the results. This protocol put an emphasis on the communication overhead cost during the verification phase, which makes him very efficient compared to other protocols.

In the next section, we will describe how to combine these different technologies into one single architecture.

PROPOSED ARCHITECTURE

The classical IoT architecture (Section II) that we have introduced previously will be used as the foundation of our own architecture for smart home. We want to point out that similar architectures focusing on security and privacy for smart homes have been already proposed. For instance, in [16] the authors presented a secure IoT framework using the TLS/SSL protocol. This framework uses an Arduino board to program different sensors and uploads the data sensed into a cloud storage for accessing the connected devices in the smart home. In addition, in [17] the authors introduced a central security manager built on top of a smart home hub or gateway router, which is positioned to intercept all traffic from smart devices. However, if these propositions share some similarities with our approach, several key components and technologies differ from ours.

A. Usage scenarios

The objective of using the FL approach in a smart home context is to enable smart devices to improve their own models (which vary from one device from another) over time.

One possible use case is that these models are sent to the corresponding manufacturers' clouds on a regular basis. As a consequence, the common generic model receive an update alongside with other users models updates which are coming from different smart home but from the same device model. Once the common generic model has been updated, it can then be dispatched to each smart device, in a similar manner of the smartphone's text prediction model. Thus, not only the smart device improves based on the behaviour of its owner but also other users owning the same smart device benefit from it.

However, using the federated learning approach in this scenario will introduce additional costs over the network. In particular when an update occurs, it requires to have a network allowing access to the outside world. Afterwards, the manufacturer send an update of the common generic model to the network, which might ask for user consent before implementing the update on the device. Furthermore, the updates need to send messages in both directions (*i.e.*, smart devices to clouds and vice-versa), which increases the overall cost and it might be done more frequently than for conventional updates.

Another usage scenario could be the situation in which the objective is to improve the model of a device based on the data collected and processed by other devices. For instance, the device might be able to better personalized the service it provided and its behaviour by taking into account other contextual information collected by other devices in the smart home. In addition the FLA could also be used to improve the model used by the IDS to detect security incidents.

a) *Self-improving smart devices:* In this first scenario, we assume that all connected devices in the smart home have the capabilities and resources necessary to use the FL approach in order to improve their models. In this case, the smart devices are improving their own models by themselves. There are two important constraints in order to be able to have this type of architecture, namely to be able to apply the FL approach in each device and for the guardian to handle the communication and models updates.

b) *The guardian oversees it all:* In the second scenario, we assume that none of the connected devices in the smart home have the capabilities to use the FL approach. The device's models, in this case, are sent and stored in the guardian and are improved within it. In this scenario, the smart unit needs to communicate more with the devices to update often their models. This scenario adds also another constraint, which is that the guardian needs to be able to use the FL approach in the place of the smart devices as they do not have the capabilities and resources to do so.

c) *The hybrid home:* The third scenario is a hybrid one in which we assume that some devices in the smart home have the capabilities to use the FL method while others are not able to do so. This implies that the constraints detailed in both previous scenarios are also present in this scenario.

B. Description of IOTFLA

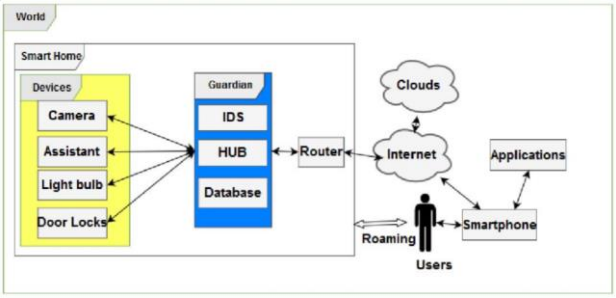

Fig. 1. IOTFLA - Overview of the architecture.

In our architecture called IOTFLA, we first introduce each basic components before diving into the use of federated learning and secure data aggregation. As illustrated in Figure 1, the smart devices first sense the data like in any other smart home scenario. Then we have three important components: (1) a HUB, (2) an intrusion detection system (IDS) and (3) a database (which is by default SQLite) responsible for storing sensible data as well as the security rules for the IDS that are merged into one single unit, which is named the *guardian*.

Finally, the architecture is also composed of a router that is connected to the network and allow devices to communicate between the smart home and the Internet but also with the external part (*i.e.*, clouds and applications) as well as the roaming users, who could be either the smart home's owners or invited guests allowed to access to the home wireless network as well as potentially some smart devices. An example could be an invited guest requiring access to the front door smart lock from the outside. Also, the smart home's owners might need to have access from the outside to the network for some applications such as a home surveillance camera or temperature controller.

For the adversary model, as in [18], we consider two type of attacks, namely local attacks and remote attacks. In local attacks, the attacker may try to ex-filtrate data or security credentials, to rely a compromised device to infect more devices, or to manipulate the information collected on the hub. In remote attacks, the adversary can gain access to the network of the devices using a malware installed on the smartphone that the user may use to communicate with the devices.

In practice, the guardian can be a dedicated computer or based on some other solutions such as Raspberry Pi 3. However, a Raspberry Pi 3 might not necessarily be able to implement all the components required for IOTFLA. The guardian capabilities should be based on the preferences, needs and also computation resources required to handle all the smart devices as well as each component within the smart home.

The HUB has a central role as the brain of the architecture, which means that it is in control of the data flows coming in and out of the smart home. Thus, it plays the role of the gateway that links the smart devices, the router and Internet (including cloud solutions) and also manage the data with the presence of a database (*i.e.*, the second main component) allowing the data to stay within the smart home while

enabling the automation of smart devices. Due to the central role of the HUB, we assume it is not corrupted by the attacker.

In practice, there are several proprietary HUBs (Samsung Smart Things, Wink Hub, Amazon Echo, Control Amy, ...) and also open-source HUBs (Home Assistant, Open HAB, Calaos, Domoticz, Open Motics, ...) available on the market. In our case, we propose to use Home Assistant, an open-source solution proposing a large panel of smart devices automation scripts. In addition, this solution has a strong and active community of developers and includes several strong security and privacy mechanisms (detailed later in this section).

The third component of the guardian is an IDS, whose role is to detect suspicious behaviour within the smart home network. For instance, it can detect when the attacker try to corrupt a device or manipulate an input. This IDS is centralized on the guardian and uses an anomaly-based approach. There are recent surveys [19], [20] that classify IDS based on common criteria such as the detection method, audit sources, infrastructure or usage frequency. For simplicity, we distinguish only between HIDS (Host-Based) in which the data collection is based on applications and system logs and NIDS (Network-Based) that are designed to monitor all local traffic within the smart home network.

The combination of the IDS and the HUB enables to have an overall better control of the data flows within the smart home network, which leads to more control over sensitive and personal data exchanges. While the IDS is used to capture anomalies and possibly detect potential attacks, the HUB operates has the gateway allowing remote access to the smart home network for the users. In the Home Assistant, several security and privacy mechanisms could be used, such as :

- *Tor* is an anonymous communication network allowing users to improve their privacy over the Internet. It encrypts and mixes internet traffic from many different sources, in which the data is wrapped into multiple encryption layers, using the public keys of the onion routers on the transmission path. However, this can result in performance issues due to increses waiting times.
- *SSL/TLS* is a security protocol creating an authenticated and encrypted channel between a client and a server, thus enabling secure data exchanges. It is based on a global trust structure that could improve confidentiality and integrity of the IoT. However, it requires a new TLS connection for each ONS delegation step, thus the search of information could be affected by additional layers.
- *Let's Encrypt* is an automated and open certificate authority managed by the *Internet Security Research Group*.
- *VPN* is a virtual private network, which is a service allowing the user to access internet safely and privately by routing the connection through a server and hiding the details of the actions performed. However, it does not allow for a dynamic global information exchange and is impractical with regard to external clients that aren't within the network.

With respect to security and privacy concerns, we suggest a security policy for the smart home environment, based on several privacy enhancing technologies [11] (some of them have been discussed previously) as well as best practice security strategies, such as:

1) Segregate the WIFI into two networks in which the first one will be the "Guest" Network, which is heavily regulated/restricted and in which clients are unable to see the devices of other clients. The second one will be the "Main" network, in which clients are able to interact with other devices through additional safety mechanisms.
2) If the smart devices are able to handle it, we recommend the use of a VPN over the "Main" network. This implies not only the knowledge of the WIFI password but also the possession of the

appropriate VPN credentials to be able to connect to the HUB and also to interact with the smart devices. This results in the data traffic being encrypted and protected from sniffers.

3) For the HUB, we suggest to only allow connections via localhost by default and always with TLS. To access remotely, a VPN is required and if the user needs external access (again it depends on the smart devices within the network), we need to ensure that only a specific IP address is allowed.
4) Implementation of a firewall and the use of IP tables to increase the security of the host.
5) Even with the previous key points, we suggest also to segregate the HUB into a DMZ network or a separate sub-network and to regulate the traffic heavily from the LAN.
6) Only allow SSH access via LAN and deny external connections entirely, the host should only allow connections via port 443 and SSH.

Now that we have defined the key components necessary to the architecture, we can move to the second part of IOTFLA in which we detail how to include the novel components into our architecture.

The first one is the FL method. Even if it is still a young approach, we strongly believe that this approach could be easily adapted for the IoT context. Indeed, there are several reasons why the FL method has gained popularity in recent years. In particular, while the centralized machine learning is the most common architecture used nowadays, the segregation between the algorithms used in clouds and the user's data spread across the world means that a large amount of personal data is always moving, which induces the following serious constraints:

- *Transfer cost*. Due to data volume growth that needs to be handled, the transfer cost can be very high.
- *Latency*. Machine learning is not the most suitable solution in many cases because it requires to interact in real time.
- *Privacy*. Transferring and storing personal data in distant servers (*i.e.*, clouds) create opportunities for hackers and augment the risk of privacy breaches.
- *Incompatibility*. Due to privacy reasons, some users are not willing to share their data on clouds.

The second component is the secure data aggregation protocol. Based on our criteria and after reducing the large available protocols to six presented in Section II-C, only two remains SecureDAV [14] and ECIPAP [15]. Both seem to fit our architecture and constraints. However, ECIPAP provides all the required criteria (confidentiality, integrity, authentication and freshness) compared to only confidentiality and integrity of SecureDAV. Thus, ECIPAP seems the best protocol for our needs, with SecureDAV being a great second option.

In addition, the FL approach has for additional benefit to limit the data communication from the smart home and the outside world (such as clouds and applications).

TOWARDS IMPLEMENTING IOTFLA

In this section, we will discuss several directions for the implementation of IOTFLA and the different designs that are available. We do realize that in its current state our proposition is theoretical and involve a high level of complexity and important implementation challenges even if each component is already being used in several deployed IoT applications.

To implement IOTFLA, we see mainly three possibilities. The first one is a fully simulated test-bed, the second a fully physical test-bed and the last one is a test-bed combining both physical components and simulated ones as proposed in [16]. Even in a simulated test-bed environment, we need smart devices, a cloud server, a computer, a router, a network, a smartphone, a database and an IDS.

Nowadays, there are several wireless sensor's networks and IoT simulators (DPWSIM, IFogsim, SinIoT, CupCarbon, Cooja, OMWNET++, NS-3, QualNet, ...) and open test-beds (Fit IOTLAB, Smart Santander, JOSE...) that are available to use for implementation purpose and that have been surveyed in [21]. However, these simulators are only necessary in a case that we want to simulate some parts or even the entirety of the IOTFLA architecture.

For this paper, we will assume a fully simulated test-bed for IOTFLA. The first step will consist in setting up the network deployment of the smart home, which include the tree deployment for the protocol ECIPAP [15], the router, the smart devices and the guardian. The guardian may be set up on a computer since the main component of the guardian is the Home Assistant solution and it is possible to deploy it on any operating system.

The second step is the setup and configuration between every component and how to connect each other. Afterwards, we would apply the basic security principles explained in Section III. At this phase, the guest network should be created such that it is heavily restricted. Afterwards, the main network could be deployed and a Virtual Private Network (*e.g.*, such as OpenVPN) added over the main network, which would enables secure access to the home and smart devices from outside.

After that, the configuration of the firewall and the IP Tables needs to be performed on the operating system to increase the security of the guardian. In addition, it is possible to segregate the guardian onto a DMZ network or a separate sub-network and then only allow SSH access via LAN. In particular, external connections are denied except for port 443 and SSH allowing applications to be used.

Once the security policy is set up, the third stage consists in setting up the automation of the smart devices with Home Assistant, which includes also the management of communications and security. Afterwards, one could use the protocol ECIPAP [15] for the secure data aggregation, which would enable us to set up the FL method. This would enable to run any of the three scenarios introduced in Section III. Afterwards, the IDS process would come into place within the unit. This would enable us to have the smart home network ready and well-functioning before connecting with the outside world such as the cloud server, roaming users and applications. Finally, we want to point out that IOTFLA can evolve or be improved by adding or upgrading different components through the years if better solutions or components are available to use in a smart home and IoT context. For example, using IoT Sentinel [18] in replacement of our own IDS or even merged both could be a potential improvement. Furthermore, techniques such as shaping, injecting, modifying traffic or even inferring behaviours [22] on smart home's network could also add an extra layer of security.

CONCLUSION

In this article, we have introduced IOTFLA, an architecture for the IoT and smart homes based on the FL method. Security and data privacy are our main objectives for IOTFLA. In order to address some of the challenges, vulnerabilities and issues [12], [13] that are common to smart home and IoT environment, IOTFLA brings two important aspects, namely (1) allowing the users to have a better understanding and control over the home network and devices and (2) to use the FL approach to improve the overall efficiency of the system over time in a privacy-preserving manner. Although IOTFLA is a rather complex architecture to implement, it represents a viable solution to answer security and data privacy challenges in a smart home context. We do hope that our proposal will inspire new developments to make smart home more private and secure.

REFERENCES

[1] K. Ashton, "That 'internet of things' thing," *RFiD Journal*, vol. 22 , no. 7, pp. 97–114, 2009.

[2] K. Hill, "Regulation (eu) 2016/679 of the european parliament and of the council," https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679, 2014, accessed: 2016-04-27.

[3] R. C. Geyer, T. Klein, and M. Nabi, "Differentially private federated learning: A client level perspective," *arXiv preprint arXiv:1712.07557*, 2017.

[4] J. Konecnˇ y,` H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[5] "Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016," https://www.gartner.com/en/newsroom/pressreleases/2017-02-07-gartner-says-8-billion-connected-things-will-be-inuse-in-2017-up-31-percent-from-2016, 2017, accessed: 2017-02-07.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5 , pp. 1125–1142, 2017.

[7] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5. IEEE, 2010, pp. V5–484.

[8] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. IEEE, 2012, pp. 257–260.

[9] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li, "A novel secure architecture for the internet of things," in *Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on*. IEEE, 2011, pp. 311–314.

[10] X. Yang, Z. Li, Z. Geng, and H. Zhang, "A multi-layer security model for internet of things," in *Internet of things*. Springer, 2012, pp. 388 – 393.

[11] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23–30, 2010.

[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks* , vol. 57, no. 10, pp. 2266–2279, 2013.

[13] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[14] A. Mahimkar and T. S. Rappaport, "Securedav: A secure data aggregation and verification protocol for sensor networks," in *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, vol. 4. Citeseer, 2004, pp. 2175–2179.

[15] L. Zhu, Z. Yang, J. Xue, and C. Guo, "An efficient confidentiality and integrity preserving aggregation protocol in wireless sensor networks,"

[16] *International Journal of Distributed Sensor Networks*, vol. 10, no. 2, p. 565480, 2014.

[17] J. M. Ibrahim, A. Karami, and F. Jafari, "A secure smart home using internet-of-things," in *Proceedings of the 9th International Conference on Information Management and Engineering*. ACM, 2017, pp. 69–74.

[18] A. K. Simpson, F. Roesner, and T. Kohno, "Securing vulnerable home iot devices with an in-hub security manager," in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 551–556.

[19] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 2177 – 2184.

[20] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[21] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[22] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of things (iot): research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2018.

[23] N. Apthorpe, D. Reisman, and N. Feamster, "Closing the blinds: Four strategies for protecting smart home privacy from network observers," *arXiv preprint arXiv:1705.06809*, 2017.