SOFTWARE DEFINED NETWORKS AS A BACKBONE FOR LARGE SCALE IOT NETWORK ARCHITECTURE FOR CRITICAL APPLICATIONS

Nair, Manas
PES University, Bangalore, India, manas.nair05@gmail.com

Jagath, Gautham
PES University, Bangalore, India, gdjk97@gmail.com

Monga, Manan
PES University, Bangalore, India, mananmonga@gmail.com

Ramachandra, Kedar
PES University, Bangalore, India, kedarramachandra@pes.edu

Abstract

The advent of Internet of Things has ushered in a new era in the internet age. Large-scale IoT networks have already become the focus for many global corporations and the number of organizations getting into the field continues to grow. However, these large-scale IoT networks have numerous inherent challenges. One of the most crucial challenges presented is securing these networks. The Software-Defined Networking paradigm has gained considerable momentum in recent times. Software-Defined networks with virtualized network functions are particularly well-suited to securing large-scale networks such as those in data centers. In this research article authors present the benefits of using a Software-Defined Networking (SDN) with virtualized network functions as a backbone for large-scale IoT networks especially networks whose infrastructures serve mission-critical applications. We analyze the security benefits offered in integrating the software defined paradigm into large-scale IoT networks and develop an architecture for the same, focused on security.

Keywords: *Internet of Things, Software-Defined Networking, Network Functions Virtualization, Security*

1. Introduction

There has been a sea of change in our daily life and working conditions in organizations with the advent of Information Technology and IT Enabled Service technologies. Developments in networking technology have allowed interconnectivity between physical devices and will invariably result in what many predict the beginning of an IoT age. The ability to program and track objects has allowed institutions to become more efficient, reduce error, minimize loss, and incorporate complex and flexible organizational systems. Realizing the potential of IoT devices, many large organizations have invested in innovation through IoT products. According to InField Solutions Inc. (2018), as of 2017, 70% of the Fortune 500 companies have already developed IoT products. The number of devices connected to the internet will only continue to grow. It is estimated that by the internet will comprise of nearly 80 billion connected devices by 2025 (Alavi *et al.* 2018). Further, the IoT paradigm has found its way into sensitive applications involving defense. Rolls Royce for instance, has incorporated intelligent sensors into their aviation system, both civil and combat to provide real time monitoring and diagnostics. Sensors on their aircraft engines use Azure Stream to transmit engine data in-flight. More specific use cases involve streaming battlefield terrain to command stations using unmanned drones and real time monitoring of equipment deployed in the battlefield. IoT devices are used in militaristic deployments for large scale projects like Fleet Monitoring in real time and inventory management using RFID sensors (Fragas-Lamas *et al.* 2016).

Every sensor transmitting data to a network, only adds to the traffic generated within the network and increases the number of potential endpoints for an intrusion. Given, large-scale IoT networks are used in critical applications, securing these networks should take top priority. Extant literature (Yu *et al.* 2015) agrees that scale of these networks and the challenges they bring with them, demand a drastically different paradigm be adopted.

Extensive literature (Bera *et al.* 2017; Bizanis *et al.* 2017; Chakrabarty *et al.* 2015; Flauzac *et al.* 2015; Gonzalez *et al.* 2016; Jararweh *et al.* 2015; Li *et al.* 2015; Tselios *et al.* 2017; Valdiveso et al. 2014; Vilata *et al.* 2016; Yu *et al.* 2015) exists surrounding the adoption of Software Defined Networking concepts into IoT networks. The Software Defined paradigm does not provide a solution to problems faced in a network. It provides flexibility by simplifying the functions of forwarding devices. Centralizing control functions allows for smoother packet forwarding, fine-grained network control and implementation of services like load-balancing and QoS based

forwarding is achieved with a reduction in costs as the network involves the deployment of simple forwarding devices.

In our paper, we present an architecture for a security network that can serve as a backbone to large-scale IoT networks that involve sensitive applications. The paper is organized as follows: Section 2 describes the Evolution of IoT Devices and provides an overview of the architecture of an IoT System. Section 3 describes security threats IoT systems face and discusses commonly employed countermeasures to stymie them. Section 4 provides an overview of Software Defined Networks. Section 5 sheds light on a priori work surrounding the field, using it as a yardstick to highlight the needs of a Software Defined Backbone Network. In Section 6 we present our architecture for a Software Defined Backbone Network. Finally, we conclude our paper in Section 7 and discusses future research and implementation steps.

2. Evolution of IoT Devices

The Internet of Things had its beginning in standalone devices like a coke machine connected to the internet at Carnegie Mellon University in 1982 and the Trojan Room Coffee Machine at the University of Cambridge connected to the internet using a Multi-Service Network Layer using an RPC Mechanism (Jun *et al.* 2011). At present, IoT has undergone an evolution from providing a platform that provides an interface to serve as a smart consumer gadget to being used alongside Big Data to become the backbone of the next generation of industry as well, a new technology in its own right, Industrial Internet of Things (IIoT) and will have a huge impact on the economy in the foreseeable future. Figure 1 gives the expected growth of IoT devices and population from 2015 to 2025 showing a surge in the number of IoT devices per person from ~2 in 2015 to ~9.5 in 2025. It has all been made possible by the evolution of cloud computing, remote storage, batteries getting cheaper and smaller allowing sensors economical and practical to fit into almost everything. It will help industries optimize their operations, implement predictive strategies for maintenance, understand large quantities of data and make decisions in real-time with a perspective that was never possible before.

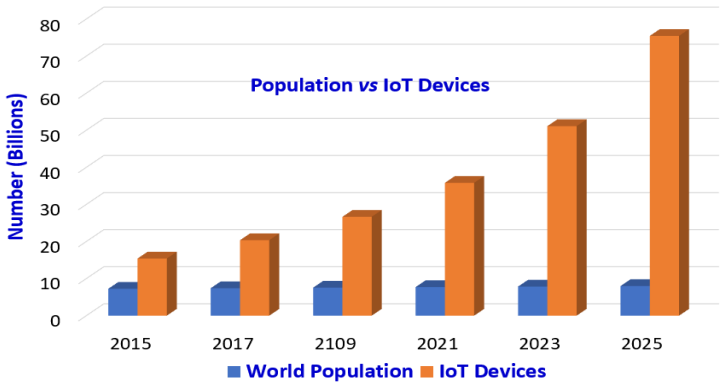

Figure 1. Growth of IoT devices with respect to population (Alavi et al. 2018)

2.1 IoT Architecture

Of the many reference models for IoT proposed, we have chosen (Li *et al.* 2015) as a reference to elucidate our own. IoT bridges the gap between the physical and digital world through the cyberspace. IoT architecture can be envisioned as three layers namely **Service Layer**, **Network Layer** and **Sensing Layer** as shown in Figure 2. The Service Layer is composed of massive data centers and servers where analysis, storage of data and applications takes place. The Network Layer consist of forwarding devices which handle routing of data from gateways to the Service Layer. The Sensing Layer includes sensors, actuators and other devices tasked with the collection of data. These devices sense and collect data from their environment and transmit them to the gateways using lightweight protocols such as MQTT (Message Queuing Telemetry Transport), CoAP, AMQ, and Websocket

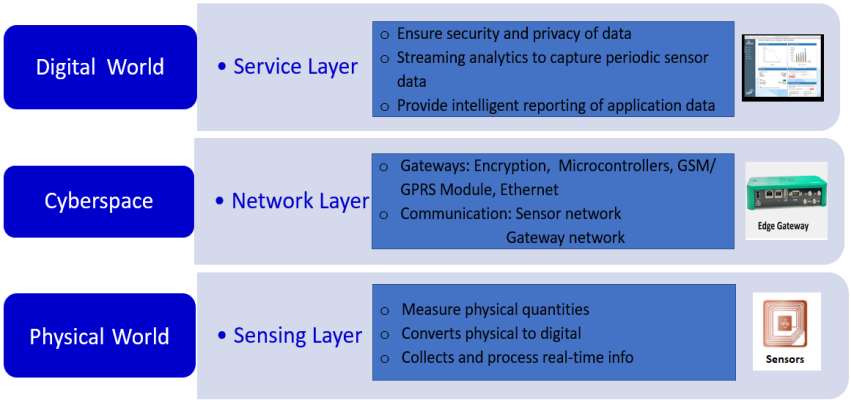

Figure 2. Conceptual View of IoT Architecture

3. IoT System Security

Data security is one of the biggest concerns with IoT technology in both commercial and sensitive military applications. Smaller IoT networks can be made highly resistant to outside attacks. However, in larger networks, the connectivity between multitudes of devices pose numerous challenges and inherent complexities. While IoT networks bare similarities to conventional computer networks, researchers are coming to terms that traditional security mechanisms like firewalls and intrusion detection systems are not adequate. One of the most organized methods of intrusion is the decomposition of IoT technology into layers and the analysis of possible intrusions in individual layers.

Threats classified by extant literature (Kamrani *et al.* 2016; Suo *et al.* 2012; Zhao and Ge 2013) fall into three sub-classes that correspond to the layers of an IoT system. Figure 3 summaries the security risks in the three layers and the countermeasures.

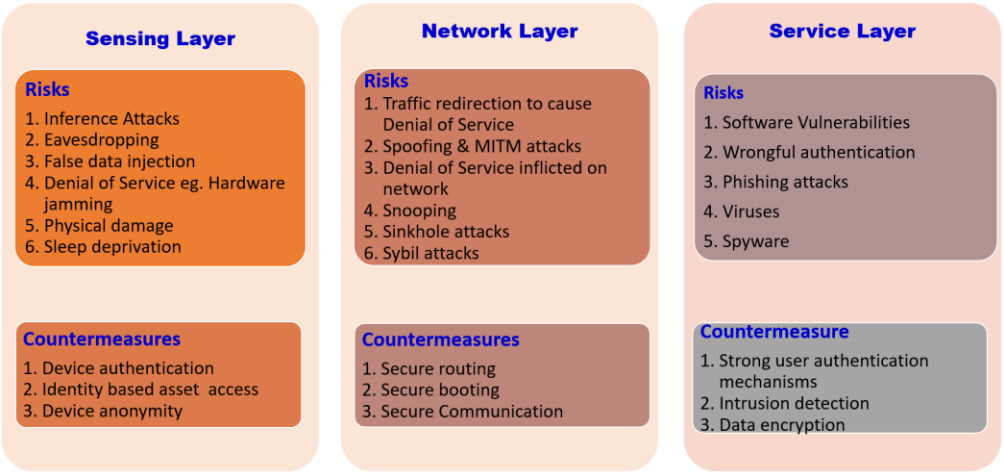

Figure 3. Security Risks in an IoT Infrastructure and their Countermeasures

3.1 Security Risks in the Sensing Layer

The sensing layer is responsible for data collection from a large number of sensors. Any disruption in the flow of data from the sensing layer constitutes a risk. The scale of the threat can vary from a minor threat like disabling a node to larger one like a Denial of Service attack to disrupt the entire application layer. Sikder *et al.* (2018) broadly classify threats to the Sensing layer into four categories. The first, Information Leakage involves inference of data from sensory input to deduce sensitive information like passwords. An example is using accelerometer vector data to infer keyboard strokes. The second form of attack involves transmitting malicious sensor commands. The

third class of attacks are False Data Injection which include node hijacking. The final class of attacks are Denial of Service attacks meant to disrupt the flow of sensor data into the IoT network, e.g. hardware jamming. A sophisticated form of DoS is a sleep deprivation attack where a node is sent messages that prevents it from going to sleep, increasing battery expenditure. Even physical damage to sensory nodes is a security risk. Perimeter defense systems will not be helpful in since IoT devices are usually deep within a network. Mechanisms to thwart these risks include device authentication, secure booting mechanisms and introducing device anonymity.

3.2 Security Risks in the Networking Layer

In large scale, mission critical IoT networks, the Networking Layer is responsible for transporting highly sensitive data. Thus, it is very important to ensure confidentiality, integrity and authenticity of data at this layer. The major concerns at the networking layer are (1) traffic redirection with intent of causing Denial of Service in a botnet attack, (2) identity spoofing, (3)Man-in-the-Middle Attacks involving manipulation of intercepted data, (4) Denial of Service against the network itself, (5) traffic snooping, (6) sinkhole attacks wherein all network traffic is redirected to a malicious node and (7) sybil attacks where forged identities of devices effect perceived changes on the network (Rajan *et al.* 2017).

3.3 Security Risks in the Service Layer

Risks at the service layer involve shortcomings in system software where vulnerabilities in the software are targeted using malware like trojans and viruses. The malware can prove to be damaging by either causing significant harm to the network's infrastructure or by siphoning out sensitive data to a malicious actor. They also involve risks such as wrongful user authentication. Even targeted attacks like spear-phishing attacks pose threats to the service layer. Security measures taken to secure the application layer are conventional mechanisms like strong user authentication mechanisms, intrusion detection and data encryption.

Our paper focuses on developing an architecture to secure an IoT infrastructures networking layer using the SDN paradigm. An SDN architecture can prove to be a good candidate to solve the resource management needs of an IoT environment. An SDN based network infrastructure reduces the complexities involved in network administration as a consequence of decoupling the network's control plane and data plane. Low-level functionalities undergo a translation into higher-level network services. Further, using the Software Defined paradigm allows balance to be achieved between centralized control via the network controller and decentralized operations realized by flow-based routing and rescheduling in the networking infrastructure.

The SDN architecture we wish to implement focuses on securing the network layer with the underlying assumption that risks from other layers are minimized by security implemented at the gateways. Along with security, the new solution must be able to support heterogenous protocols, software and hardware.

4. Software Defined Networks

Traditional computer networks consist of networking devices like switches and routers along with devices responsible for controlling traffic like firewalls with complex protocols implemented on them. Networking functions are implemented by configuring network policies on these devices which then translate them into configuration commands to process forwarding of the data they receive. The devices are largely abstracted into black boxes. In Software Defined Networks (SDN), the "network intelligence is logically centralized in software-based controllers" (Nunes *et al.* 2014) in the control plane, and network devices become simple packet forwarding devices constituting the data plane. The control and data plane in traditional routing devices are decoupled. The centralized controller communicates with forwarding elements using a Southbound protocol like OpenFlow and the controllers are programmed by network administrators using service APIs. While Software Defined Networks may be associated with a centralized networking structure, they in fact allow for decentralization to be introduced since the controller architecture can be distributed. Further, using a controller for network access allows for fine-grained control over data moving through the network since forwarding devices do not deal with the processing overhead incurred when providing for QoS, service guarantees and network policies. The Software Defined provides flexibility when delegating security features and granular control over policies administered. For instance, it allows Network Function Virtualization (NFV) wherein physical firewalls are abstracted into virtual firewalls. In the next section, we discuss previously presented solutions for SDN based solutions to IoT networks.

5. SDN SECURITY FRAMEWORK FOR IOT

IoT devices are vulnerable to security risks in heterogeneous networks. Flauzac *et al.* (2015) propose envisioning the IoT system as an ad-hoc network where every node has a built-in OpenFlow compatible switch. Nodes without these switches are connected to a neighboring node

with one. Each SDN sub-network has a root controller referred to as a Border Controller. When a node establishes a connection with a Border Controller all its ports are blocked, and the device is authenticated. Following authentication, the node downloads flow entries from the controller. Border controllers act as security guards and exchange information regarding security policies implemented in their domain. When devices from different domains need to contact each other, border controllers are responsible for mediating communication.

A second implementation involved Black SDN networks for IoT (Chakrabarty *et al.* 2015) which incorporated security into the Link layer and the Network layer. The architecture involved building the entire network infrastructure and protocols from the ground up. The robust design ensures attackers are cannot snoop in and learn details like source and destination address and frame number. Secure routing mechanisms like Random Routing Scheme, Dummy Packet Injection Scheme and Anonymous Communication Scheme (ACS), Anonymous Path Routing (APR), Simple Anonymity Scheme, Destination Controlled Anonymous Routing Protocol for Sensor nets (DCARPS) and Hashing Based Identity Randomization are used for this. All packets in the network have a time to live value (TTL) and packets are dropped or destroyed within this frame of time. IoT devices are simulated as nodes. Each node has its own address and sleep pattern which may vary. A problem that may arise is that sometimes packets may not reach their intended destination because intermediate nodes are asleep. The SDN controller then manipulates flow tables to ensure packets are sent via a route with awake. The controller with a view of the entire network, is best placed to find an optimal route. It can also activate nodes for transmission using encrypted control messages.

In securing the network, one ensures a secure core for the IoT network's infrastructure. Gonzalez *et al.* (2016) propose grouping larger scale IoT networks into clusters. Each cluster is then designated with a cluster-head (termed SDNCH) given capability to direct flow messages to switches and notify other cluster heads they are in communication with of devices on their network. The controllers implement security policies and the distributed controller architecture is referred to as Distributed Smart Firewall (DISFIRE). The authors propose using Cisco's policy based OpFlex as an alternative to OpenFlow.

Yu, Sekar et al posit that (1) host-based approaches are ineffective and suggest network-based solutions, since IoT devices contain a significant number of unpatched vulnerabilities and have

limited resources; (2) traditional static perimeter defenses are inadequate since devices are deployed deep within networks, and their physical and computational contexts constantly change. The solution they posit follows that of a Software Defined Framework. In the process of decoupling the data plane from the control plane they introduce separate security modules termed as µmboxes responsible for performing security checks as a more pervasive form of conventional security mechanisms like honeypots. They also suggest schemes like incentivizing and anonymizing bug reports to improve security.

It needs to be noted that a more practical approach to designing a network that serves as a backbone to a large scale IoT network will be to develop a secure network infrastructure to which IoT nodes may be added since larger IoT networks employ edge devices from multiple vendors who focus on functionality over security. However, provisions should exist for installing software patches on edge devices. SDN in our architecture will serve to unify complexity, scalability and security.

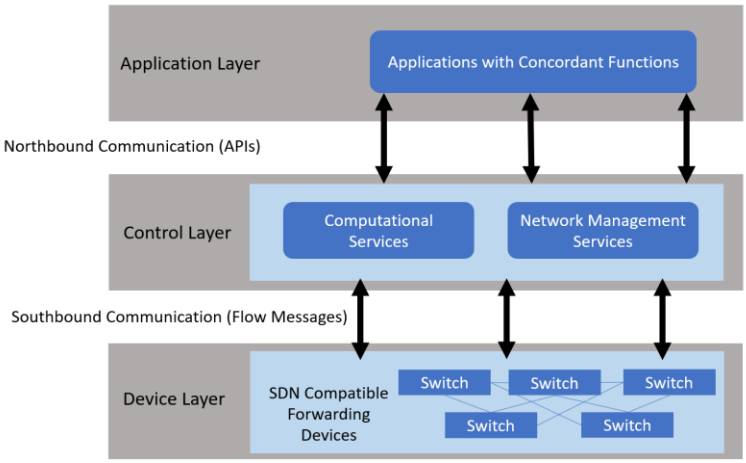

Figure 4. SDN Architecture

6. Proposed Architecture

The philosophy that our architecture follows is that the backbone network should allow for IoT edge devices, possibly from different vendors to be seamlessly integrated as they would into a traditional network. The architecture we propose follows a traditional three-layered model. The lowest layer is the **sensing layer**, where sensors collect a large amount of data in different

formats for different applications. The devices collect information and forward them to gateways responsible for performing pre-processing and pushing them onto either the cloud or another part for the network for processing. The gateway also implements security checks on the devices connected to them and the data it receives.

The **network layer** differs from traditional network layers in IoT networks in that we use the Software Defined paradigm where the control plane and the data plane are decoupled. Network tasks like load balancing and maintenance of Quality of Service will be implemented in this layer. We implement network security features by introducing controllers responsible for data forwarding and designating security policies. The network layer comprises of SDN controllers and forwarding devices which forward data based on flow entries received from SDN controllers. We propose giving IoT gateways power to program the forwarding devices when devices across sub-clusters need to communicate with each other. The SDN controllers communicate with forwarding devices using Southbound APIs. Controllers communicate amongst themselves using East-Westbound APIs. The controllers use Northbound APIs to communicate with the network's application layer which is a part of the infrastructure's **service layer**, an umbrella term for all interfaces with the network. The aspects of network security we implement are:

6.1 Controller Hierarchy

We propose introducing a hierarchy into SDN controllers distributed across the network. In addition to providing fine-grained control and a globalized view over the network, we are given more control over the security of the network allowing smoother management of compromised controllers. We provide the distributed network of controllers with a tag corresponding to their level on the hierarchy (ID0, ID1, ID2 and so on). The ID tag will correspond to security features inherent to the controller such as the level of encryption and processing power of the controller. Controllers higher up in the architecture are given the ability to overwrite flow rules written by controllers with a lower status in the hierarchy.

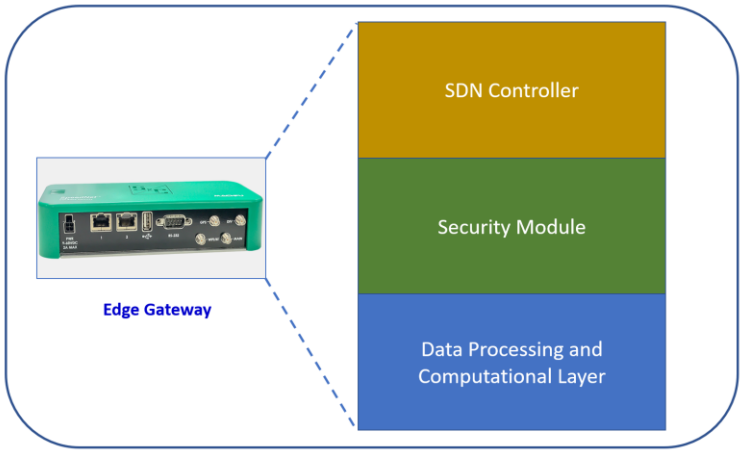

Figure 5. Cluster Gateway

6.2 Gateway level security

Most IoT implementations involve implementing network level security features at the host level itself. However, we need to address that host-based solutions are lacking in their fluidity due the limited resources nodes possess. Unique solutions tailor-made to the network's use case are required. To this end, we implement security modules embedded within gateways. These security modules are responsible for implementing network security functions and can be customized for specific devices and their usage. They should be rapidly deployable and reconfigurable on change of environment. The security modules implemented are responsible for ensuring the veracity of devices connected to them. We suggest performing randomized deep packet scans on traffic sent to the gateways to inspect for malware by analyzing signatures. Further, gateways provide abstraction to the centralized controller about the nature of the devices connected to them and can homogenize the nature of data being sent from them.

6.3 Centralized Controller

We introduce a centralized controller that is given a view of all gateways and controllers on the network. It will be given significant processing power and be made highly secure and resistant to attack. It will sit at the top of the controller hierarchy and be given the ability to overwrite flow rules written by any other controller on the network. The centralized controller will monitor the gateways and consider the different devices, the environment in which they function and develops a plan for the enforcement of security policies for different devices which are then

pushed onto the security gateways. Further, processing of reports provided by the intrusion detection system is done at this centralized controller.

6.4 Anomaly based Intrusion Detection System to Monitor Controllers

Security provided at the gateway layer allows for the reasonable assumption that data received from the sensing layer does not pose a threat to the networking layer. However, controllers on the network themselves must be monitored for possible intrusion. Since, an infiltrated controller will attempt to reprogram flows on switches within the network, an anomaly-based Intrusion Detection System should be able to detect a misbehaving controller. The IDS must then send its compiled reports to the centralized controller which can then reclaim the compromised device by performing a hard reset on the device.

6.5 Redundant Controllers

SDN controllers capable of determining flows and deploying security features are expendable if we assume that the centralized controller is not as susceptible to attack. So, rather than focus on securing SDN controllers lower in the hierarchy which might prove to be expensive, we suggest introducing redundant controllers which are monitored by the anomaly-based IDS present in the network. If a controller is compromised, the centralized controller will deactivate it by overwriting rules written by the compromised controller. The centralized controller should then perform a hard reset of the compromised controller. Having more controllers than necessary will ensure that in the event of compromise, the network can function unmitigated.

6.6 Inclusion of Ad-Hoc networks

An ad-hoc network typically consists of sensors or nodes divided into clusters. Each cluster then has a cluster-head node, statically or dynamically assigned depending on the use case. In our architecture, we propose having cluster heads forward all data to a pre-programmed gateway. Here, sensor data is converted to a single format suitable for transmission across the network. The gateway determines where to forward the data and can programs flows to redirect the data if required.

6.7 Distributed Firewalls

The distributed firewall mechanism we propose follows the one described by Pena and Yu (2014). Packet filtering firewalls used in OpenFlow environment is taken as a starting prototype. All packets pass switches with virtualized firewalls to reach their destination. The firewall listens

for arriving packets which check whether the packet headers match rules set. If a rule listed by the firewall is not met, the packet is dropped. Rules are stored as flow entries on the switch. If no matching flow entry exists, the packet is forwarded to the controller which decides where to send it by querying the flow tables of other switches or drops it. The priorities of the firewall flow entries are set to maximum. Rules are installed into every forwarding device connected to the network as programmed at the application layer.

One possible avenue for attack is attempting intrusion at the centralized controller to gain control over the entire network. However, recent advances in decentralized networking technologies like the blockchain have shown the possibility of using consensus mechanism to ensure multiple centralized controllers working in unison. A risk analysis between adopting a decentralized, distributed central controller system versus securing the central controller with state-of-the-art security features needs to be performed.

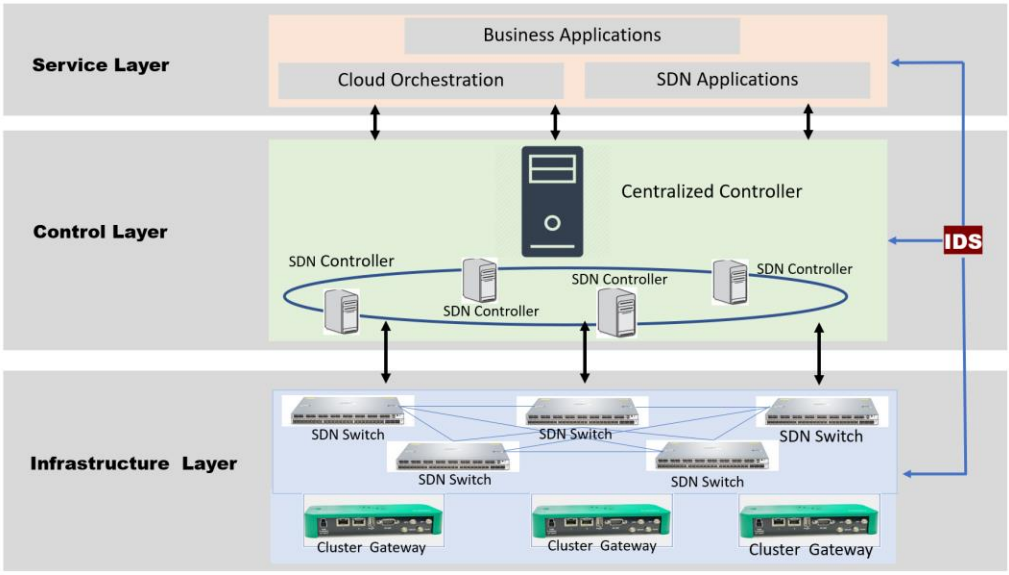

Figure 6. Proposed Architecture

7. CONCLUSION

In our paper, we discussed the challenges faced in large-scale IoT networks that often transmit sensitive data and presented the security risks these networks face. Breaches in modern-day IoT networks can result in huge losses and we provided a framework for a secure networking core to these networks. Our architecture was designed keeping in mind that most IoT networks rely on plug and play devices from multiple vendors and followed the philosophy that these devices

should be seemingly seamlessly integrated into our network. We plan on taking our work forward by studying the feasibility of our proposed architecture by implementing the same. We intend to use the OpenDaylight controller to serve as the controller for our architecture and at present, intend to use the Mininet emulator to represent the underlying Data Plane.

REFERENCES

Alavi, A. H., Jiao, P., Buttlar, W. G., & Lajnef, N. (2018).” Internet of Things-Enabled Smart Cities: State-of-the-Art and Future Trends”. *Measurement* 129, 589-606.

Bera, S.,Misra, S. and Vasilakos,A. V. (2017). “Software-Defined Networking for Internet of Things: A Survey”. *IEEE Internet of Things Journal* , 4 (6), 1994-2008.

Bizanis,N. and Kuipers,F. A. (2016). “SDN and Virtualization Solutions for the Internet of Things: A Survey”.*IEEE Access*, (4) 5591-5606.

Chakrabarty,S., Engels,D. W. and Thathapudi,S. (2015). “Black SDN for the Internet of Things”.In: *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems* , 190-198.

Flauzac, O., Gonzalez, C., Hachani, A. and Nolot, F. (2015). “SDN Based Architecture for IoT and Improvement of the Security”.In: *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops* , 688-693.

Fraga-Lamas, P., Fernández-Caramés, T., Suárez-Albela, M., Castedo, L. and González-López, M., 2016. A review on internet of things for defense and public safety. *Sensors*, *16*(10), p.1644.

Gonzalez, C., Charfadine, S. M., Flauzac, O., and Nolot, F. (2016). “SDN-based security framework for the IoT in distributed grid”. *2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, 1-5.

InField Solutions Inc. (2018).*Internet of Things Infographic*.URL:http://infieldsolutionsinc.com/2017/09/08/internet-of-things-infographic/ [Visited on 01/10/2019].

Jararweh, Y., Al-Ayyoub, M., Benkhelifa, E., Vouk, M. and Rindos, A. (2015). “SDIoT: a software defined based internet of things framework”. *Journal of Ambient Intelligence and Humanized Computing*, 6(4), 453-461.

Jun, Z., Simplot-Ryl, D., Bisdikian, C. and Mouftah, H.T. (2011). “The internet of things”. *IEEE Communications Magazine*, 49(11), 30-31.

Kamrani, F., Wedlin, M., Rodhe, I. (2016). “Internet of Things: Security and Privacy Issues”. *FOI Swedish Defence Research Agency, Defence and Security, Systems and Technology*.

Li,J. , Altman,E. ,Touati,C. (2015). “A General SDN-based IoT Framework with NVF Implementation”. *ZTE Communications*, 13 (3), 42-45.

Nunes, B.A.A., Mendonca, M., Nguyen, X.N., Obraczka, K. and Turletti, T. (2014). “A survey of software-defined networking: Past, present, and future of programmable networks”. *IEEE Communications Surveys & Tutorials* ,16 (3) 1617-1634.

Pena, J. G. V., and Yu, W. E. (2014). “Development of a distributed firewall using software defined networking technology”. In: *2014 4th IEEE International Conference on Information Science and Technology*, 449-452.

Rajan, A., Jithish, J., & Sankaran, S. (2017). “Sybil attack in IOT: Modelling and defenses”.In: *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) ,* 2323-2327.

Sikder, A.K., Petracca, G., Aksu, H., Jaeger, T. and Uluagac, A.S. (2018). “A survey on sensor-based threats to internet-of-things (iot) devices and applications”. *arXiv preprint arXiv:1802.02041*.

Suo,H., Wan,J., Zou,C. and Liu,J. (2012)."Security in the Internet of Things: A Review".In: *2012 International Conference on Computer Science and Electronics Engineering* ,648-651.

Tselios, C., Politis, I. and Kotsopoulos, S. (2017). “Enhancing SDN security for IoT-related deployments through blockchain”. In: *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)* ,303-308.

Valdivieso Caraguay, A.L., Benito Peral, A., Barona Lopez, L.I. and Garcia Villalba, L.J. (2014). “SDN: Evolution and opportunities in the development IoT applications”. *International Journal of Distributed Sensor Networks*, 10(5), p.735142.

Vilalta, R., Mayoral, A., Pubill, D., Casellas, R., Martínez, R., Serra, J. and Muñoz, R. (2016). “End-to-end SDN orchestration of IoT services using an SDN/NFV-enabled edge node”. In: *Optical Fiber Communications Conference and Exhibition (OFC)*, 1-3.

Yu, T., Sekar, V., Seshan, S., Agarwal, Y. and Xu, C. (2015). “Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things”. In: *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV* .New York:ACM ,p.5.

Zhao, K. and Ge, L. (2013). “A survey on the internet of things security”. In: *2013 Ninth international conference on computational intelligence and security*,663-667.