American Journal of Agricultural Science Engineering and Technology

ISSN: 2158-8104 (Online), 2164-0920 (Print)

Volume: 5, Issue: 1

Published by: e-Palli, Florida, USA

The American Journal of Agricultural Science, Engineering and Technology (AJASET) is blind peer reviewed international journal publishing articles that emphasize research, development and application within the fields of agricultural science, engineering and technology. The AJASET covers all areas of Agricultural Science, Engineering and Technology, publishing original research articles. The AJASET reviews article within approximately two weeks of submission and publishes accepted articles online immediately upon receiving the final versions.

Published Media: ISSN: 2158-8104 (Online), 2164-0920 (Print).

Frequency: 2 issues per year (January, July)

Area of publication: Agricultural Science, Engineering and Technology. The subjects covered by the journal includes but not limited

Agriculture
Agricultural Economics and Agri-business
Agricultural Engineering
Agricultural Statistics
Agricultural Extension and Development
Agro-forestry and Ecotourism
Agronomy
Agro-tourism
Animal Science and Nutrition
Applied Agriculture
Applied Economics and Finance
Aquaculture
Bioinformatics
Biotechnology and Biochemistry Climate Change and Green Technology
Collaborative Engineering
Computer Science and Engineering
Computational Biology
Crop Science and Production
Dairy Science & Poultry Science Decision Support System
Entomology
Environmental Science and Extension
Dental and Medical Science
Experimental Agriculture
Food science, Engineering and Technology Genetics Technology
Geophysics
GIS, GPS, and Remote Sensing
Horticultural Science
ICT for Agricultural Development
Irrigation and Water Resource Engineering Land Use and Development
Mathematics
Modeling of Crop and Animal System
Pathology and Plant Protection
Fisheries
Plant Breeding and Crop Science
Post-harvesting Technique and Technology Precision Agriculture
Production Engineering
Social Science and Agricultural Development Soil Science
Tropical Agriculture
Veterinary Science and Technology

to:

AN ONTOLOGICAL SECURITY FRAMEWORK TO SECURE THE SDN BASED IOT NETWORKS

Nazmul Hossain[1], Md. Zobayer Hossain[2] and Dr. Md. Alam Hossain[3*]

DOI: https://doi.org/10.5281/zenodo.4701562

ABSTRACT

The IoT (Internet of Things) is now a trendy technology with its numerous apps in multiple areas. It includes a heterogeneous amount of Internet and mutually linked devices. Since the IoT network is characterized by tiny assets that produce less energy and are more flexible, this number of machines is difficult to monitor. SDN (Software Defined Network) is a new network model that facilitates the creation and introduction of fresh networking abstractions, simplifies the management of network and facilitates network development. In this paper, by leveraging the fundamental characteristics represented by Software Defined Networks (SDN), we present an ontological security architecture for IoT networks. Our security architecture restricts access to independently verified IoT devices via the network. To secure the flows in the IoT network infrastructure, we introduced an extra layer and provide a lightweight protocol to authenticate IoT systems. Such an advanced strategy to protection containing IoT device authentication and allowing approved flows can assist secure IoT networks against malicious IoT devices and threats.

Keywords: Internet of Things (IoT) Security, Software Defined Network (SDN); IoT Security; SDN IoT Model.

[1]Assistant Professor, Department of Computer Science and engineering, Jashore University of Science & Technology, Jashore-7408, Bangladesh, email: n.hossain@just.edu.bd

[2]Department of Computer Science and engineering, Jashore University of Science & Technology,Jashore-7408, Bangladesh, email: zobayer130127@gmail.com

[3]Associate Professor, Department of Computer Science and engineering, Jashore University of Science & Technology Jashore-7408, Bangladesh.

* Corresponding Author, email: alam@just.edu.bd

I. INTRODUCTION

The concept of Internet of Things was introduced given the large number of machines and items linked to the Internet as well as linked to each other. The Internet of Things (IoT) uses multiple equipment and techniques to detect, communicate, measure and report real-world data needed to improve the quality of life.

Multiple fields such as smart cities, medical care, transport, supply chain, agriculture, automation, etc. many comparable applications have been donated and packaged under IoT. The IoT produced smart physical stuff by incorporating a number of complex detectors, actuators as well as controllers to benefit the environment and even how we reside and connect with our surroundings. As a solution, all these things and items produce enormous information collected through sensing and tracking of things. By the assistance of machine learning and AI, extremely precise predictions and choices are produced, reliable information and data analysis techniques data mining and big data are also used to evaluate these data without manual assistance. SDN is the recent programmable strategy and network concepts that distinguish the data plane from the control plane. Controls, monitors and automatically alters the behavior of the network by generating direction software on the system.

Since the SDN framework relies on the divergence of control plane and data plane, it offers flexibility and scalability in network management and set-up, and even the implementation of legislation and practices that are implemented interactively and dynamically via a central operating plane.

With their multiple requirements, the number of Internet-related smart objects is expected to exceed 50 billion phones by 2020. These heterogeneous systems are considered to be IoT components that will need to be efficiently addressed and installed. Each device requires individual programming when upgrading and altering equipment, which means absorbing more time and energy and improving the cycle of evolution. Hence, finding alternatives to these problems and being more adaptable and reprogrammable to configure / reconfigure and program / reprogram systems. Whereas IoT has been designed for a wide range of devices as well as limited data packets, SDN is the perfect option for IoT versatility to fix transition by quickly attaching an enormous number of devices. One of SDN's primary characteristics is that it does not require any single device's individual setup. A centralized controller performs this setup. In addition, SDN retains mobility, virtualization and management of resources. IoT and SDN are both evolving communication technologies. It should be coupled with other techniques such as SDN to keep IoT intelligence. In a standard manner, SDN supports many kinds of service requirements. In this context, as both are new subjects, they were given more attention to the option of mixing them, either academic or industrial.

In this paper, we describe an architecture of ontological security using SDN for an infrastructure of an IoT network. The security architecture utilizes a safety procedure created to control and handle facilities and IoT devices as well as to safeguard the respective flows in the IoT infrastructure. For example, strategies can implement safe data channels from specific authenticated IoT devices via specific cloud gateways. This can lead to secure IoT network infrastructure flow management. Our security architecture also offers IoT utilities enabled for device authentication and data authenticity as well as network service device authorization. Open Authorization (OAuth) protocol can be used to obtain authorization for network

services required by individual IoT devices. Using an integrated SDN controller, the suggested architecture was introduced.

II. FANDAMENTALS OF IoT AND SDN

In IoT, all appliances and items are linked to the Internet in separate aspects than humans can. Things can be in the form of uniquely identified and connected physical objects or virtual objects. Those IoT sensing devices / objects retrieve, deliver, obtain, manage, communicate, store and analyze information. The nature of IoT isn't just monitoring devices, but there are also many items connected to the network and interacting among each other which are governed by various network designs and protocols. 2018 4th International Communication and Automation Conference (ICCCA) 978-1-5386-6947-1/18/$31.00 © 2018 IEEE 1A.

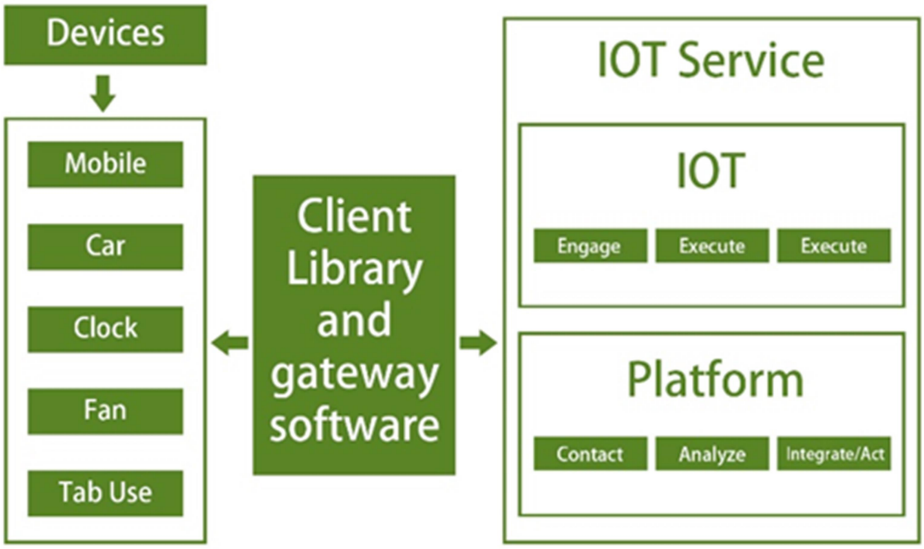


Figure 1: A traditional Architecture of IoT

It has proposed and suggested many architectures and models for IoT. As most of the architectures are suggested researchers as three layers / domains as shown in the figure 1, there are four layers of other proposed architectures.

A. IoT Architecture consists of the following layers:

Perception layer: This is the part of physical hardware's such as sensors and actuators. It's also known as the layer of perspective and equipment's. It is ultimately accountable for the detection, collection and transmission of information from border Sensors for network devices, like sinks or gateways.

Network layer: in this layer are presented all communication techniques used in IoT, like Bluetooth, Wi-Fi or cell phones. The transmission of information collected by physical objects in the sensing layer is performed by the system domain layer.

Application and service layer: It measures and analyzes all information gathered in the device layer such as located in the cloud and servers. All IoT applications and facilities were included in the said layer, depending on the client/system specifications.

Middleware layer: Since IoT systems and applications are supplied by different producers and interact with each other, and likewise without thinking regarding equipment and supplier data, it was accomplished by middleware, which is regarded targeting and process governance.

Now at second, Software-defined Network (SDN) is an evolving network paradigm that makes it possible to change traditional constraints on network infrastructure. It removes the order of conventional network designs by separating command and therefore data plane, too. Network appliances as well as routers and switches are transmitted only and distributed surveillance is carried out logically. Recently, SDN has been operating all cloud computing environments and servers, and it can form the foundation of most anticipated network systems. Major suppliers of network systems like Cisco, Juniper, and Huawei have physically and virtually joined SDN capabilities to many of their latest network equipment, which can now function both physically and virtually. SDN also delivers control planes with different inputs to ensure accuracy, effectiveness and scalability.

B. SDN Architecture as follows:

Network systems and equipment in a legacy network monitoring as well as

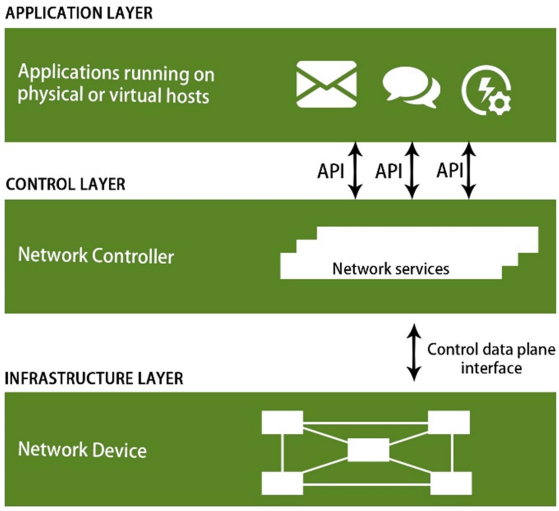


Figure 2: Three layered Architecture of SDN

data plane are accessible in each computer, resulting in complex configuration and installation of recent

systems and evaluation of system components. SDN disconnects and divides the control plane from the data plane. All network devices were also transmitting devices just, as well as the controller is logically centralized for managing the network. The controller sends updates

and guidelines to all transmitting equipment via suitable APIs for all configuration and control options.

The SDN architecture composed of 3 layers that interact through Northbound and Southbound APIs between each other. These 3 layers are shown in Figure 2 and are defined as follows:

Data layer: It provides network transmission devices, like switches, routers, etc., which transmit traffic on the basis of orders and rules, which are described by a centrally controlled controller. The data layer is often referred to as the infrastructure layer, the forwarding layer and also the device layer, respectively.

Control layer: The whole portion is often named the SDN controller. It is being treated also as brain of the network. The SDN controller is essential for transmission of information decisions. It offers programmability by establishing directions and guidelines for managing and controlling the network, as well as dynamically debugging equipment remotely. The controller is regarded as SDN's critical part. Controller generates network settings and defines guidelines and rules on the basis of network prerequisites. The SDN controller must have an international perception of the entire network and total ownership across all parts of the network.

Application layer: It demonstrates most network systems and programs which satisfy the expectations of the consumer. These apps interact through Northbound APIs with the controller.

In addition, to interact between layers and elements, SDN has different APIs. Southbound, Northbound, Westbound, and Eastbound are these APIs. There is comprehensive Southbound API communication between controller and forwarding equipment wherein the different regulations could be applied to systems like switches and routers on a data plane. The most widely used instance of the Southbound API is the OpenFlow standard. Northbound is often used as an interface for system applications. It enables communication among vice versa, as well as providing the network perspective of the Northbound API to the application layer. Numerous controllers must be in place to coordinate choices and connect to one another on the Westbound and Eastbound APIs for more redundancy.

III. SDN BASED IoT

The IoT network protocols and their existing design were not developed to support enormous amounts of information, flexibility and robustness. There are some constraints to serve as well as manage this diverse interconnected device that produces an enormous amount of data. SDN is regarded to be the new technology best suited to meet IoT's versatility, robustness and complementarity requirements. IoT's development as well as evolution in protocols, architectures, techniques, and leadership is going on very fast.

In SDN, the network framework had also changed from static to intelligent and configurable as an option. In order to eliminate network congestion, SDN provides an intelligent SDN routing controller with such a wide perspective of the network as well as the probability of transmitting data where necessary. In addition, SDN integration simplifies IoT mechanisms for data processing and decision-making. Furthermore, SDN offers multiple debugging instruments that can be used in IoT systems to improving the capacity of the network to

collect data. Numerous domains such as smart transport, microgrid systems and smart home have also identified the advantages of combining SDN and IoT. As latest, its convergence with certain other network services and solutions produces a study gap. In this part, IoT solutions based on SDN will be discussed in numerous ways.

Hakiri et al have introduced an IoT architecture which incorporates with SDN to allow usability and information sharing among IoT devices connected to the SDN facilitated IoT gateway. The SDN controller connects with IoT applications via the Middleware Publishing/Subscribing Data Delivery Service (DDS) and the Southbound API forwarding systems. Researchers highlight a number of difficulties and problems, like mobility, usability, integration and quality of service (QoS).

Riekki et al. suggested an effective SDN-based IoT architecture. The architecture composed of four layers: layer of devices, layer of communication, layer of computing, and layer of service. Figure 3 shows this architecture.

Device layer: the first layer consists of actuators and sensing equipment used to monitor adjacent environments and to collect information for different apps and services in different 3 formats. In addition, some of the appliances in this layer, such as actuators, execute certain duties as per the network commands given.

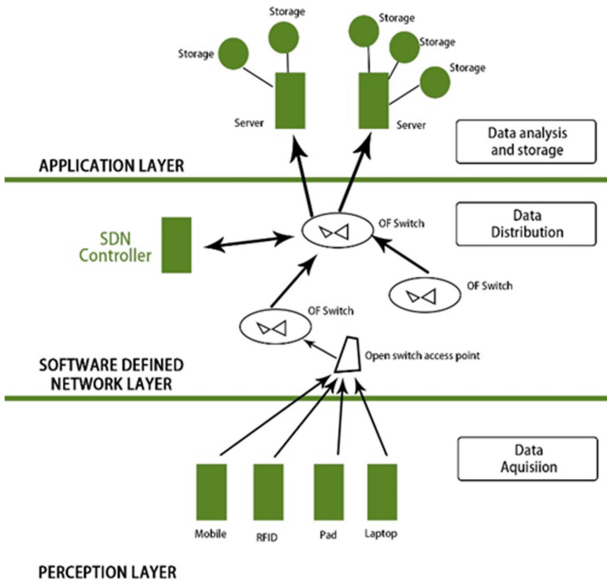


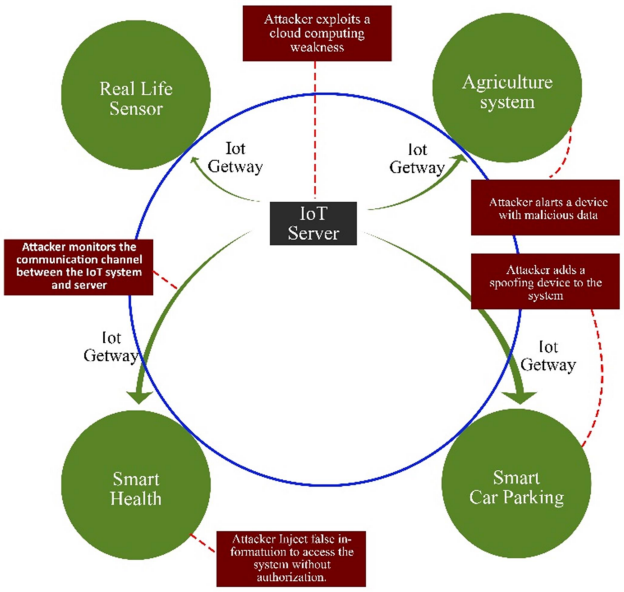
Figure 3: SDN based IoT layered Architecture

Communication layer: In this communication layer are situated the equipment used for the transmission of information like router and SDN gateways.

Computing layer: The SDN controller is consolidated in the computing layer, that monitors the transmission of data involving various facilities and their needs. As well as managing activities, maintenance, safety, IoT services, hardware, and topology, SDN controller is liable. In addition, the computation layer includes accounting and accounting methods.

Service layer: It is the layer containing the IoT services and apps developed to meet the requirements. Services and apps are programmed through SDN controller programming in this layer.

The researchers concentrate completely on IoT architecture based on current network implementation and scale of the network, lack of reusability and integration. The top layer



relies with servers offering IoT app APIs, while the Network Operating System (NOS) and SDN controllers are located in the middle layer. The south layer is made up of IoT gateway and the middle layer of connected SDN network switches. Researchers have justified their recommended IoT network improvement structure, and a network operating system needs to be built to understand the different IoT devices. In our proposed model, we operate with the architecture of Riekki et al. and secure the IoT networks based on SDN.

IV. SECURITY AND MANAGEMENT CHALLENGES IN IoT

One of the most significant elements of the full implementation of the Internet of Things in the actual world is security. Many IoT systems ' heterogeneous connectivity conveys several difficulties and potential threats. In fact, IoT protection raises the responsibility of privacy specialists as it includes the provision of privacy services to billions of smart objects.

Figure 4: Threats and challenges of IoT in real life scenarios

One of the primary problems to be discussed when considering the future of IoT protection is the large amount of occurrences with IoT technologies. In IoT systems, there's many threats, such as spoofing, traffic sniffing, complex data manipulation, code injections, illegitimate access, etc., as shown in Figure 4. At various stages in time in the IoT environment, attacks can happen, which prioritizes the significance of data securityAs shown by Wolf and Serpanos, those structures must be intended and operated from a unified view of privacy and security characteristics as they handle several times the physical environment and vital activities. IoT security includes the underlying complexity of IoT, further aggravated by

numerous heterogeneous data exchanges among models and IoT tools. Those devices appear to be progressively exposed to the Www, which poses an ever-changing risk of current threats and privacy problems not yet found.

Another challenge in the IoT-based framework is the absence of awareness of security's fundamental components: resources, threats, methods of security, weaknesses and characteristics of security. In order to prevent intrusions from the physical and virtual world, different IoT devices involve separate protection processes. In all other words, a violated IoT device could be regarded as an access point for malicious users to gather sensitive user data leading to the destruction of two privacy features: integrity and data privacy.

The idea of IoT protection could therefore get crucial, influencing IoT implementation in various fields. Indeed, Dell's 2016 study discovered that security experts were 49 percent more susceptible to spending even many times to secure their data with appropriate information when they correctly understand the security problems and threats.

In order to mitigate particular threats, there are several traditional safety mechanisms and facilities. Even so, the use of smart IoT devices enables the collection and processing of data from sensors without taking into consideration these processes. In many cases, IoT equipment's and sensors implemented to execute tasks without taking into consideration potential vulnerabilities, leaving them open for eavesdropping, hammering, manipulation, jamming, etc.

Those possible security flaws mentioned above have a significant effect on IoT settings. To tackle these threats to IoT security, our proposal follows an illustration which will be used across the document to demonstrate the solutions proposed: "The IoT setting is often susceptible to Wi-Fi attacks and is easily targeted due to misconfigured terminals, data infringement and DoS. Use of a weak cryptographic algorithm without having cryptographic integrity protection, as in the Wired Equivalent Privacy (WEP) scenario, erodes protection for WLAN. Our aim is to introduce a new strategy to enhancing IoT safety based on SDN using network to identify and process monitoring and classify flaws withinin a base and apply appropriate security syatem designed for specific threats.

V. PROPOSED ONTOLOGICAL SECURITY FRAMEWORK TO SECURE SDN BASED IoT NETWORKS

As demonstrated in our hypothesis, the IoT network security framework is an important requirement for enterprise, academia and public stakeholders to totally adopt the Internet of Things. To connect and use properly, it is necessary to define the security-relevant features of the IoT devices. Security procedures are crucial to home and enterprise and comprise a factor that enterprises have not yet properly considered in the context of their method of risk management. In our paper, it proposes a model of ontological security based on the IoT security dimension. Our goal is to introduce a new approach to enhancing SDN-based IoT protection and concentrating on observing, analyzing and classifying security pitfalls in a base, whereas allowing for the following threat-adjusted privacy service delivery, improve security techniques for business applications and technological resources. To all this end, we propose divide the structure into four layers and integrating a layer dealing with security, respectively, as well as an integration layer used by communication and computation layer (see Figure 5). The network and system monitoring methods collect security alerts from

multiple security tools that define and classify baseline circumstances of interest (e.g., attacks and security flaws). The linked ontological layer can offer appropriate security services in IoT settings using such understanding and its reasoning processes.

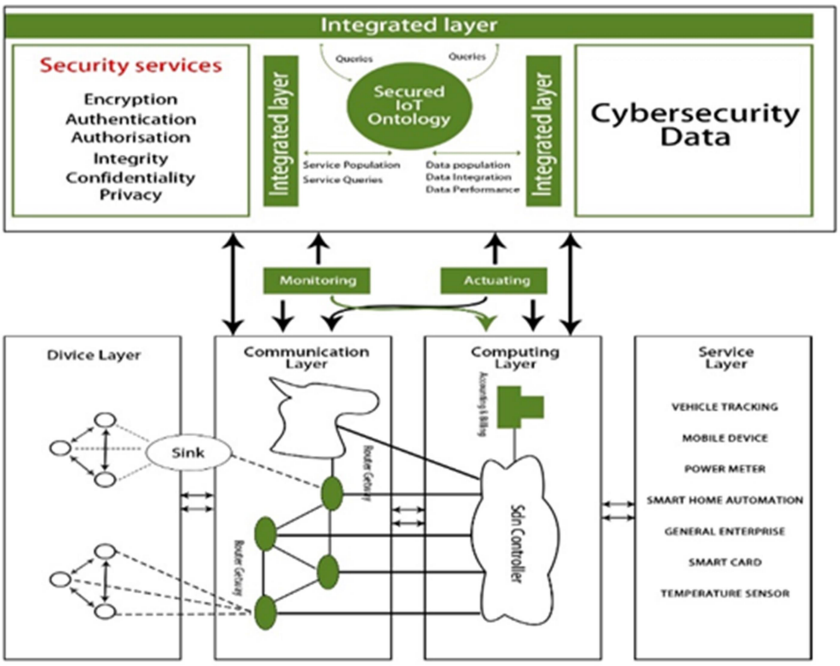


Figure 5: Proposed Ontological framework

The integrated block provides data analysis and traffic information from ontology and access to multiple privacy services concerning multiple enterprise procedures and network devices; measures to ensure threat-free safety systems. The following sections define in detail these blocks.

The monitoring and actuating blocks of the network and process offers two additional techniques for exploring the system: monitoring and actuation. That first method is based on monitoring situations of concern in each system that are being analyzed. This involves detecting potential intrusions, theft of data, viruses, ransomware, etc. Monitoring tools provide information on different types of privacy warnings that are then tested using distinct security tools like firewalls, intrusion detection systems, vulnerability scanners, etc. Each scenario is then examined to determine if proper techniques exist that can be implemented to recover the system and enhance security at that given time. The second method focuses on these adaptations, i.e. according to the security analysis, to prevent threats arising from the integrated layer's IoT base. It includes of implementing suitable methods or modifying specific protocols in order to prevent detected security threats.

This IoT security base is considered by the integrated layer of the proposed system to execute data integration in a unified database with separate information sources. Using ontological reasoning, the correlation between the primary ontology classes offers implicit data from services available in the integration layer to give appropriate security alternatives. The integration layer offers data from pre-build safety facilities that can be created from service design and adaptation either externally or at design moment.

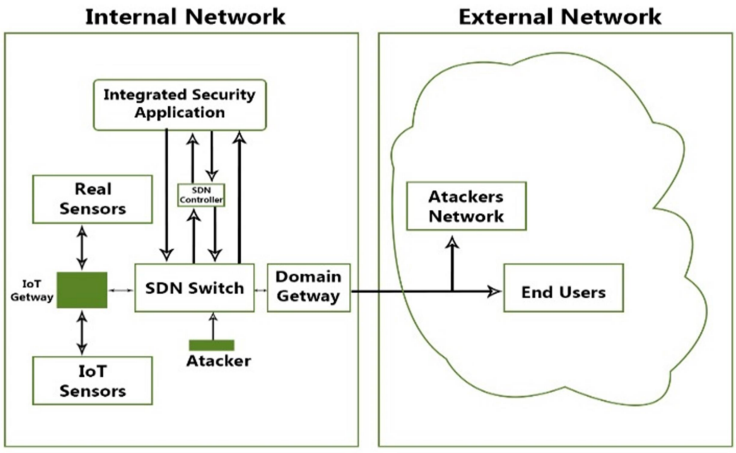


Figure 6: Experimental Network Topology

To implement our design decisions, we have set up a reconfigurable test platform. Our proposed structure is split into two parts as shown in this figure 6:

A. Internal Network

- A firewall function for Linux
- SDN stack: built-in SDN controller
- IoT stack: supports approximately 6 Wi-Fi and altered stacking the middleware process network protocols, allowed SDN OF.
- Sensors for IoT Network: 4–6 physical sensors, 2 workstations operating a virtual simulation of IoT devices, runs all protocols of Wi-Fi.
- Attack of IoT: It is a simulator software tool generating attacks, blurring procedures and the network jamming.
- Common attacks: Here uses a collection of computers operating the commonly used attack instruments and exploit kits.
- Integrated Security Applications: Runs cryptographic algorithms, customized security procedures, authentication system, integrity protocols etc.

B. External Network

- Sets some valid hosts and users and services to access our IoT test network using TCP/IP protocol suit.
- Attacking host users, botnet apps accessing TCP / IP covert channels, generating DoS attacks and focused IoT network testing for malware intelligence gathering or information stealing.

VI. VALIDATION AND PROOF OF PROPOSED ONTOLOGICAL SECURITY FRAMEWORK

This chapter discusses what IoT safety issues, specifications, threats and attacks are handled by the suggested security structure. Figure 7 Summarizes the services that the suggested framework fulfills. The graph helps to evaluate which modules meet the security demands, challenges and threats of IoT in the network mentioned previously in the proposed scheme.

This chapter also introduces the ontology validation using a SQuaRE standards methodology to define its weaknesses and strengths.

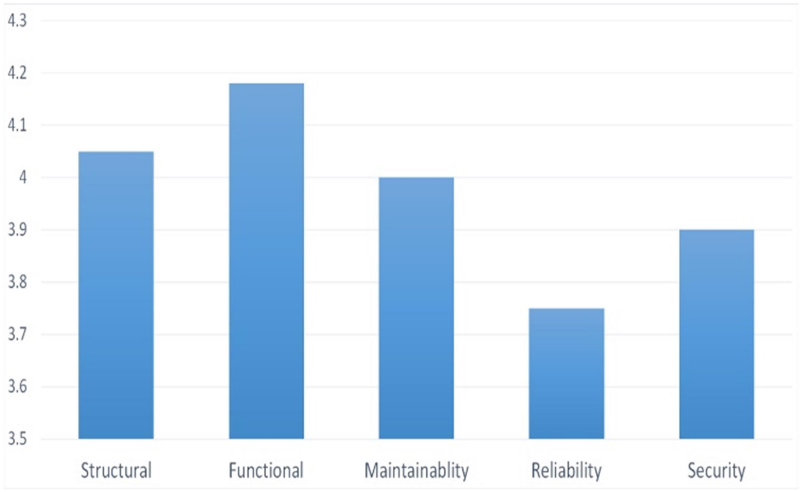


Figure 7: Graphical representation and score of proposed Ontological Framework

The ontological framework contains the security domain using the framework against potential vulnerabilities and threats on the fundamental elements of security. This analysis is based on a methodology. The adopted ontology analysis methodology was intended to adapt the OQuaRE framework software engineering standard. This proposal was submitted to support designers identify weaknesses and strengths in accordance with SQuaRE standards using a sequence of ontology quality features. For the ontology analysis, the model reuses the SQuaRE features, namely: structural, functional, maintainability, reliability, and security. Figure shows the evaluation results achieved for ontology quality features:

- The first scenario is structural properties. It is one of the semantic and formal ontological characteristics which is commonly used in modern approaches to analyze. It is a complete consistency with outstanding domain protection. It allows verify fields those are closer to each other. As a result of collecting information from distinct sources, it illustrates in the IoT base. The relationship of the amount of properties and interactions provides a comparatively small value under structural features to the help of formal relationships, that can be enhanced by using the laws of interpretation which maintains better formal interactions.
- The second feature is functional properties which follows such criteria depending on the theme of fulfillment of requirements of functional properties for distinct reasons. The assessment showed coherent search and query and reuse of information as its strengths, taking into account the average amount related interactions, the number of characteristics each class, and the area of the route from the leaves to the object. Though, weaknesses connected with the amount of cases were proved by a sub-characteristic. This element has no effect on the analysis because ontology needs a full information population for real-world implementation.
- The feature of maintainability offers the capacity of ontologies to adapt in case of demands or functional requirements to modifications in settings. The number of

characteristics also affects the maintenance because a very specific ontology allows it more portable to know.

- The features of reliability match to the ontology maintenance of the performance level for a specified time span under the stated conditions.
- The security feature matches info like security vulnerabilities and threats that uses ontology within a current security class. This involves detecting potential intrusions, theft of data, viruses, ransomware, etc. Monitoring instruments provide data about various kinds of privacy threats which is then explored by using separate security instruments like as firewalls, attack detection procedures, vulnerability metrics etc. Each scenario is evaluated to classify whether there are exact solutions that can be implemented at that particular time to recover the system and enhance security.

Figure 8: Graphical representation of Global Average score of proposed Ontological Framework

The results shown above illustrates the ontology's strengths and weaknesses. The global average score can be found to have a value of 3.98 showed in Figure 8. Some characteristic has been affected by specific quality metrics; the overall quality of our proposed model is still better. It requires some progress in the future which could produce a better result in accordance with the human evaluation criteria.

VII. CONCLUTION AND FUTURE WORK

Development in programmable networks has allowed a new SDN paradigm that has opened network security opportunities. The IoT paradigm of emerging interconnected embedded devices is distinct from standard wired networks that are generally resource-constrained. Managing such networks therefore presents difficulties of a specific nature. This paper identifies and discusses IoT security difficulties and proposes a noble architecture to secure the SDN based IoT networks. IoT discusses security threats, attacks, challenges and requirements that need researchers ' attention. SDN's IoT development potential has been investigated recently. There is no doubt that the SDN paradigm provides an outstanding chance to ensure IoT safety as security control is centralized.

The proposal discussed in our paper given a standard technical structure for monitoring and mitigating IoT application processes and technology resources using IoT security domain ontology. Some contributions to enhance security surveillance, analysis, as well as service design and provisioning can be outlined at this point to highlight specific asset limitations in an industrial setting. One of these contributions is Ontology, which collected security understanding about alerts and potential threats from qualitative security problems data to correlate vulnerabilities and security characteristics. Key components of IoT security were linked by the correlation between classes: assets, threats, security mechanisms, vulnerabilities, and security characteristics. Ultimately, how the suggested SDN-based framework addresses the security attacks and threats in IoT. The suggested module will be physically introduced and assessed in the context of general overhead costs and resource consumption in the future.

REFERENCES

A. Carie, M. Li, S. Anamalamudi, S. B. Shah, and W. Khan, "AnInternet of Software Defined Cognitive Radio Ad-hoc Networksbased on Directional Antenna for Smart Environments," SustainableCities and Society. 2017.

A. Duque-Ramos, M. Boeker, L. Jansen, S. Schulz, M. Iniesta, J. T. Fernández-Breis, "Evaluating the Good Ontology Design Guideline (GoodOD) with the Ontology Quality Requirements and Evaluation Method and Metrics (OQuaRE)." PLoS ONE 2014, 9, 1–14.

A. El-Mougy, M. Ibnkahla, and L. Hegazy, "Software-defined wireless network architectures for the Internet-of-Things," in Proceedings - Conference on Local Computer Networks, LCN, 2015, vol. 2015–Decem, pp. 804–811.

A. H. Shamsan, A. R. Faridi. "SDNAssisted IoT Architecture: A Review", 2018 4th International Conference on Computing Communication and Automation (ICCCA), 2018

A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications," IEEE Commun. Mag., vol. 53, no. 9, pp. 48–54, 2015.

A. Marotta, F. Martinelli, S. Nanni, A. Orlando,A. Yautsiukhin, "Cyber-insurance survey." Comput. Sci. Rev. 2017, 24, 35–61.

Dell Data Security Survey Finds that a Lack of Security Knowledge Limits Business Initiatives. Available online: http://www.dell.com/learn/us/en/uscorp1/press-releases/dell-data-security-survey/ (accessed on 4 August 2019).

D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things Security: a top-down survey," Comput. Networks, vol. 0, pp. 1–24, 2018.

D. Kreutz, F. M. V. Ramos, P. E. Verı´ssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking : A Comprehensive Survey," vol. 103, no. 1, 2015.

E. Haleplidis, J. H. Salim, and D. Meyer, "Software-Defined Networking (SDN): Layers and Architecture Terminology," pp. 1–35, 2015.

J. Li, E. Altman, and C. Touati, "A General SDN-based IoT Framework with NVF Implementation," ZTE Commun., vol. 13, no.3, pp. 42–45, 2015.

J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications." IEEE Internet Things J. 2017, 4, 1125–1142.

K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," Comput. Electr. Eng., vol. 66, pp. 353–368, 2017.

M.A. Khan, K Salah, "IoT security: Review, blockchain solutions, and open challenges." Future Gener. Comput. Syst. 2018, 82, 395–411.

M. B. Yassein, S. Aljawarneh, M. Al-Rousan, W. Mardini, and W. Al-Rashdan, "Combined software-defined network (SDN) and Internet of Things (IoT)," Electr. Comput. Technol. Appl. (ICECTA), 2017 Int. Conf., pp. 1–6, 2017.

M. Ojo, D. Adami, and S. Giordano, "An SDN-IoT architecture with NFV implementation," 2016 IEEE Globecom Work. GC Wkshps 2016 - Proc., 2016.

M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN Architectures: A Systematic Literature Review," vol. 0, no. 0, 2018.

M. Wolf, D. Serpanos," Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems." Proc. IEEE 2018, 106, 9–20.

N. Bizanis and F. A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey," IEEE Access, vol. 4, pp. 5591–5606, 2016.

N. Omnes, M. Bouillon, G. Fromentoux, and O. Le Grand, "A Programmable and Virtualized Network & IT Infrastructure for the Internet of Things," Int. Conf. Intell. Next Gener. Networks, pp. 64– 69, 2015.

S. Bera, S. Misra, and A. V. Vasilakos, "Software-Defined Networking for Internet of Things: A Survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1994–2008, 2017.

S. Khan, M. Ali, N. Sher, Y. Asim, W. Naeem, and M. Kamran, "Software-Defined Networks (SDNs) and Internet of Things (IoTs):A Qualitative Prediction for 2020," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 11, pp. 385–404, 2016.

S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software Defined Network (SDN) Based Internet of Things (IoT),"Proc. Int. Conf. Futur. Networks Distrib. Syst. - ICFNDS '17, pp. 1–8, 2017.

S. Sharma, R. Mishra, K. Singh, "A Review on Wireless Network Security. In Quality, Reliability, Security and Robustness in Heterogeneous Networks", Springer: Berlin/Heidelberg, Germany, 2013; pp. 668–681.

T. Ninikrishna et al., "Software defined IoT: Issues and challenges," Proc. Int. Conf. Comput. Methodol. Commun. ICCMC 2017, vol. 2018–Janua, no. Iccmc, pp. 723–726, 2018.

V. C.P, “Security improvement in IoT based on Software Defined Networking (SDN),” Int. J. Sci. Eng. Technol. Res., vol. 5, no. 1, pp. 291–295, 2016.

W. Suryn, A. Abran, A. April, “ ISO/IEC SQuaRE. The Second Generation of Standards for Software Product Quality. 2003.” Available online: https://www.semanticscholar.org/paper/ISO-%2F-IEC-SQuaRE-.-The-second-generation-of-for-Suryn (accessed on 6 August 2019).

Y. Li, X. Su, J. Riekki, T. Kanter, and R. Rahmani, “A SDN-based architecture for horizontal Internet of Things services,” 2016 IEEE Int. Conf. Commun. ICC 2016, 2016.

Y. Li and M. Chen, “Software-defined network function virtualization: A survey,” IEEE Access, vol. 3, 2015.

Z. Han ; X. Li ; K. Huang ; Z. Feng "A Software Defined Network-Based Security Assessment Framework for CloudIoT" IEEE Internet of Things Journal; Year: 2018 Volume: 5, Issue: 3