An IoT Framework Based on SDN and NFV for Context-Aware Security

Arlyn Verina Ong and Marnel Peradilla
Advanced Research Institute for Informatics, Computing and Networking
De La Salle University
Manila, Philippines
Email: arlyn.ong@dlsu.edu.ph, marnel.peradilla@dlsu.edu.ph

Abstract**—** The Internet of Things (IoT) connects a complex set of devices that perform data collection, processing, and environmental control in various applications. Due to the extent of potential monitoring and control capabilities, its infrastructure and data security is an essential design consideration. This presents unique challenges due to the heterogeneity of devices and dynamism involved. Context should thus be considered when applying suitable security measures without unnecessarily taxing the network. To do so, a four-layer framework that incorporates Software-defined Networking (SDN) and Network Function Virtualization (NFV) is proposed due to their flexibility in rapidly adjusting to network conditions to support context-aware security in IoT applications.

Keywords—Internet of Things, NFV, SDN, security, context

I. Introduction

It is envisioned that over the next few decades, there will be an exponential growth of devices that connect to the Internet [1]. These devices can be computers or everyday objects that take the role of sensors that capture data from the environment, actuators that control the environment, those that store data, and those that perform data processing to extract meaningful information. Networking technologies along with application services allow these devices to interact with each other, creating a complex infrastructure that has the potential to automate various tasks and provide a wealth of information. This vision of the future Internet is currently known as the Internet of Things (IoT), a network that connects uniquely identifiable devices to the Internet that offers advanced services through its interconnectivity made possible by interoperable communication methods [2] [3].

As devices in the IoT become highly connected, generating and processing large amounts of data, and transmitting these across different networks, there is a need to ensure sufficient security measures to protect the confidentiality of potentially sensitive personal information as well as the integrity and availability of device operations [4] [5] [6] [7]. Security for traditional networks has always been a challenge. The same can be said for the IoT, and perhaps at an even higher degree due to the heterogeneity of devices that can be connected and its potential pervasiveness. Further complicating this is the dynamic nature of the IoT. It is a system that will be constantly changing [3]. Depending on the IoT application, devices may join or leave the network at any time, move from one location to another, and generate data of varying types and importance. Given this, traditional security measures which often rely on static configurations and rules to safeguard a network may not provide an adequate amount of flexibility and responsiveness to cope with the security and data delivery requirements of such a dynamic network [8].

For a network to intelligently determine and apply a suitable set of security measures without severely impacting network performance, it must consider the type of data being carried and the circumstances in which data is generated. It must also be supported by an infrastructure that offers the capability to dynamically alter network behavior without the need for constant human intervention to exact changes across many devices [9].

Software-defined networking (SDN) and Network Function Virtualization (NFV) are potential solutions for these requirements. SDNs are a networking paradigm that allows networking functions to be controlled by applications to achieve flexibility, rather than by traditional dedicated networking devices [10]. NFV on the other hand, uses virtualization technology to provide on-demand, scalable and flexible deployment of network functions as virtual appliances instead of using security hardware [8]. Together, these two technologies may introduce a large degree of adaptability to the network through the processing of context inputs, dynamically provisioning the network functions, and perform the traffic forwarding necessary to meet security requirements.

This paper explores the use of SDN coupled with NFV to implement context-aware security in the IoT. Succeeding sections discuss the security considerations in the IoT, the definition of context and its role in IoT security, how SDNs and NFVs can be used to address IoT security, and a proposed framework to use of SDNs and NFV capabilities guided by context-awareness to protect IoT data.

II. Security Considerations

To understand how context can significantly influence security measures applied to the IoT, one must first delve into some key characteristics of the IoT that have a large impact on security considerations in the network.

A. Pervasiveness

The devices of the IoT may be present in various applications, be it in healthcare, environment monitoring, disaster response, transportation, industrial automation and

978-1-7281-6476-2/21/$31.00 ©2021 IEEE

more. These devices may be present in any aspect of the environment that even everyday objects can be made capable of interfacing with a network [11] – collecting different types of data to monitor the environment. These environments are often open as well. IoT devices may be deployed in public locations which offer minimal physical protection to devices from potential tampering [12].

While each sensor may seem mundane based solely on the data it gathers, it can potentially contribute to building a very detailed picture of the monitored environment or object when processed into information together with data gathered by other sensors. Because of this, data privacy and confidentiality issues need to be considered [13] [14]. Furthermore, actuators can be used to control various aspects of the environment, some of which have a direct impact on human safety. In this aspect, access control and integrity of data fed to actuators are equally important as well.

B. Heterogeneity

The IoT is composed of several types of devices - each serving a different purpose, built using different hardware platforms and communicating via different network technologies and protocols, [2] [3] [4]. These can range from fully functional devices with computing capabilities such as a PC or a mobile phone, but may also be built as lightweight devices such as Arduino and Intel Galileo boards, and embedded hardware platform such as those found in IP-enabled appliances [15].

One of the primary issues is that IoT devices may be made available with existing vulnerabilities but with limited built-in security mechanisms, and have closed firmware, giving the customer no other option but to rely on external security measures to protect them. Additionally, the use of lightweight devices with limited computing resources also limits the options for security measures that can be supported. Traditional IT security is targeted for use with resource-rich devices. IoT devices, on the other hand, may have to rely on more lightweight security measures, while striking a balance between the level of protection and resource utilization [12]. A wide variety of devices, with different capabilities, using different technology and producing different types of data all contribute to the complexity of implementing protective mechanisms. Using a single type of security technology is unlikely to be effective.

C. Scale

The number of devices that are envisioned to be connected to the future Internet is envisioned to far exceed the scale of the current state of the Internet [3] [4]. It is predicted that, around 21 billion devices will be connected to the Internet by the year 2025 [16]; and communications triggered by these devices will be an order of magnitude larger compared to human-triggered communication as well. The numerous devices, coupled with their heterogeneity offer a large attack surface that needs to be adequately protected; and at the same time, the large volume of data involved requires proper management and handling [12]. With the potentially huge amount of data transmissions that occur at any time among the devices involved in an IoT application, any implemented security measures and technologies must be adequately robust and resilient in order to avoid introducing a significant performance impact and becoming a single point-of-failure in the network.

D. Dynamism

With new devices and applications that grow exponentially, the IoT is a system that continues to expand and change dynamically [3]. This includes device status, connectivity, identity, location, as well as circumstances. Depending on the IoT application, devices may join or leave the network at any time, move from one location to another, and generate data of varying types and importance. With these, the IoT is expected to be a complex entity in which security requirements for a given device or a given data transfer changes regularly. Traditional methods of providing security which often rely on static rules or configurations are not suitable for this type of deployment [17]. Measures that are designed to be tight and complex for potential high-security situations may needlessly constrain operations at a time when a simple unprotected data transfer will suffice. On the other hand, measures that are designed to be laxer to reduce resource utilization may provide inadequate protection when the need to transfer sensitive data arises.

III. Definition of Context in the IoT

According to de Matos et al [17], context refers to any high-level information that can be used to characterize the situation of an entity. This can refer to various aspects surrounding an event in an IoT system, which in general, may be summarized into the 4 W's which can potentially have bearing on what security measures are best suited for enforcement in an IoT application.

These 4 W's represent a general idea of the possible elements to include when characterizing events in an IoT application that can influence security measures that need to be applied. Each of these may be further interpreted or aggregated into more specific information to give an even more detailed set of characteristics – such as age, and historical behavior to describe a person, similar to [18]. Using these information to adjust security measures automatically is advantageous in a dynamic and heterogeneous system such as an IoT. As new events change the state of an IoT application, security policies and levels also change in response to address potential threats. This is what is defined as context-aware security [19].

A. Who

The 'Who' context refers to persons involved in the IoT event which can include the one who initiates a data transfer and the person that the data may pertain or belong to. These have implications to access control based on privileges of the person performing the action, as well as the use of privacy-preserving measures that may be needed to protect the identity of the person that the data describes. As an example, traffic management staff may be authorized to view traffic conditions and common travel routes of vehicles in a smart city application; but should not be allowed to associate a specific travel route to a specific person.

B. What

The 'What' context refers to the identity of devices involved in the event and the content of data being transmitted in the network. Given the heterogeneity of devices in the IoT network, it is important to determine the nature of the devices where data originates and is destined for based on their capabilities and role in the application. Capabilities of IoT devices have a direct effect on the type of security measure they can support such as whether a mainstream approach can be used, or a lightweight alternative is needed. At the same time, the role of each device in the application affects access control measures applied to it. Those that trigger and perform events that affect human safety (such as opening doors) may need more stringent control compared to those that do not (turning on lights).

The content of data is also an aspect to consider due to its effect on how its transmission needs to be handled. Sensitive data may require means to preserve their confidentiality; and critical data may require integrity verification to trigger security responses when anomalous content is detected.

C. Where

The 'Where' context may be used to indicate the location where a certain device is deployed. Depending on location, a device in a public or unprotected location is more prone to tempering and may need to employ security measures that allow verification of data integrity versus one that is deployed in relatively secure private premises. Also, this context indicates where a device is triggered or where the monitored object is located, which affects access control measures that permit or deny an action based on user authority. For example, an actuator controlling a lock for an external door will need stricter access control rules compared to one inside a house.

D. When

The 'When' context can indicate the time of day which, like location, can have implications on access control measures on a device that are driven by rules that check critical hours when devices are used or when events happen. It can also be used to determine when an event occurs relative to another event. In applications such as in [20], sequences of data received from different devices are used to gain a complete picture of an event occurring within the monitored environment. Depending on the sensitivity of the application, security monitoring for any anomalous behavior in the environment can be implemented.

IV. SDN AND NFV IN IOT

To create a security infrastructure that can cope with changing policies, adaptive technologies capable of dynamically altering data traffic flow and deploying security devices as needed by the application need to be employed. This section explores how SDN and NFV can fill this requirement for an IoT application with context-aware security.

A. Network Function Virtualization

NFV leverages virtualization technology to decouple software from the hardware [21]. Using NFV, network services may be provisioned on-demand as software on general-purpose hardware. Fig.1 shows the NFV architecture.

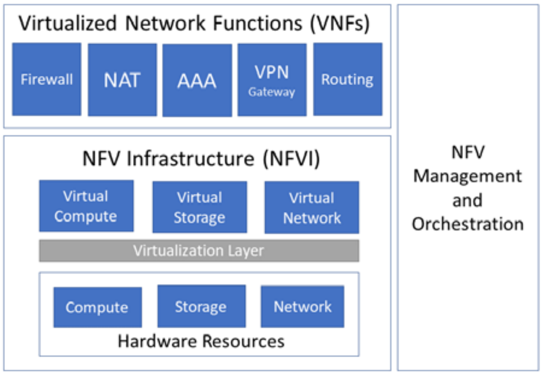

Fig. 1 NFV high-level architectural framework [22]

A set of Virtual Network Functions (VNF) encompass a wide variety of services that are commonly found as dedicated appliances in a traditional network. These include switching functions such as routers or Network Address Translation (NAT) devices, security functions such as firewalls, AAA servers and IDS, VPN gateways, and more. The Network Function Virtualization Infrastructure (NFVI) is comprised of the physical computing resources which include computing power, storage, and networking, as well as virtualization technology such as hypervisors needed to host the VNFs.

These components are controlled by the NFV Management or Orchestration block which hosts services that onboard and catalog available VNFs; coordinate their set-up, migration, and tear-down according to needs; and allocate and reclaim physical resources throughput the lifecycle of instantiated VNFs. When applied to security in the IoT, the capability of NFV to separate software from hardware allows security services to run on different devices ranging from general-purpose to single-board computers. This flexibility means that there is no need for dedicated physical equipment to provide security services, and that these services may be instantiated anywhere and anytime according to need based on context information. Furthermore, dynamic service provisioning also makes it possible to quickly deploy, scale, or tear down these services alongside varying network conditions.

B. Software Defined Networks

SDNs allow networking functions to be controlled by applications, rather than by management consoles that control individual devices found in traditional networking. To accomplish this, SDNs use a layered architecture as illustrated in Fig. 2.

In an SDN, the infrastructure layer is composed of hardware devices or virtual switches referred to as forwarders which function only to move data packets. Network intelligence and data forwarding decisions are made at the control layer usually by a central controller which pushes data

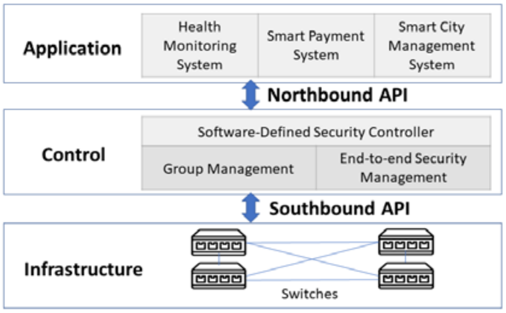

Fig. 2 Software-defined networking layered architecture [23]

forwarding policies via a southbound interface to forwarders using a communication protocol and specific commands that define a set of data packet characteristics to match, defined as a flow, and the corresponding action to be performed by the forwarder [24][25] Finally, the application layer refers to any network application that uses the SDN for data communications. To convey specific data forwarding needs to the network, the application must communicate with the Control layer via a northbound interface, usually an API [26].

The layered architecture promotes flexibility in that networking functions are no longer constrained to any specific hardware device or location in the network. Any forwarder may function as a firewall, gateway, or custom device based on data flow handling instructions from the controller [26]. Using a central, intelligent controller promotes manageability and agility. Changes in network requirements or operations no longer involve manual reconfiguration on several network devices as this requires adjustments to be made only to the controller, which will then push the necessary flow changes through southbound communication to forwarders.

The programmability of SDN allows an IoT application to manipulate network operations in real-time by defining the behavior it expects from the network using the SDN northbound API [27]. This capability further promotes flexibility because of the potential to automate various tasks by programming these into the controller using the API. It is through this programmability that an SDN can be made to adapt to changing contexts by altering traffic flow to specific appliances hosting a virtualized network security function according to defined policies without the need for manual intervention [28] [29].

V. Proposed Framework

Given the flexibility and dynamic capabilities of both NFV and SDN, both technologies can be harnessed and integrated to build a network architecture suitable for a context-aware IoT application. NFV can dynamically provision security functions where suitable according to the context inferred from collected information; while SDN technology can redirect the path of traffic to instantiated network functions as needed. A proposed architecture of such network is illustrated in Fig. 3 and is composed of four distinct layers.

A. Device Layer

The device layer refers to the physical end devices that make up the application. Among these are IoT devices which may include installed sensors, wearables, and actuators; personal user devices such as personal computers and mobile devices; as well as generic nodes, typically servers, which host images containing VNFs or serve as computing resources to run these VNFs on-demand.

VNFs can include various services used by the network and application (e.g. web, DHCP, message brokers, etc). More importantly, the VNFs should include security enforcement and support services. These are VPN gateways that can enforce privacy, AAA services to provide user or device identity verification, permission and activity logging, firewalls for traffic filtering beyond packet header inspection, and intrusion detection systems. Data collected from sensors and user devices as well as control commands to actuators can be forwarded among devices in this layer as through the network infrastructure represented by the connectivity layer.

B. Connectivity Layer

The connectivity layer refers to the physical infrastructure that provides network connections between hosts in the device layer. Essential to this layer are SDN switches whose flow tables can be modified dynamically to forward data packets to the appropriate devices, such as NFVI nodes when security policies and application context call for such.

Depending on the types of devices included in the application, gateways may be needed to interface IoT devices that use non-IP protocols such as Bluetooth or Zigbee to the rest of the IP network. Wireless access points may also be included for 802.11-based devices to be connected. In such cases, the IoT gateways and wireless access points would need to be connected to the SDN switches so that their traffic flow can still be manipulated by higher control layers.

C. Network Control Layer

The network control layer provides the manipulation of the network traffic flow and the security services provide in order to match context requirements. Given this, the elements found in this layer would be the NFV management and orchestration modules and the SDN controller.

The NFV management and orchestration modules takes VNF images from repositories according to the security services needed by the policies invoked by contexts, provisioning them on the NFVI nodes, monitoring them, and managing physical resources on the nodes to the individual VNF depending on demand. It must provide the catalog of available VNFs and their capabilities to the upper layer so that the VNFs can be correctly matched to the requirements of the data flow or transactions occurring within the IoT application.

The SDN controller can manipulate flow tables of SDN switches so that traffic flows needing security services can be diverted to the NFVI nodes hosting the security VNFs. Since

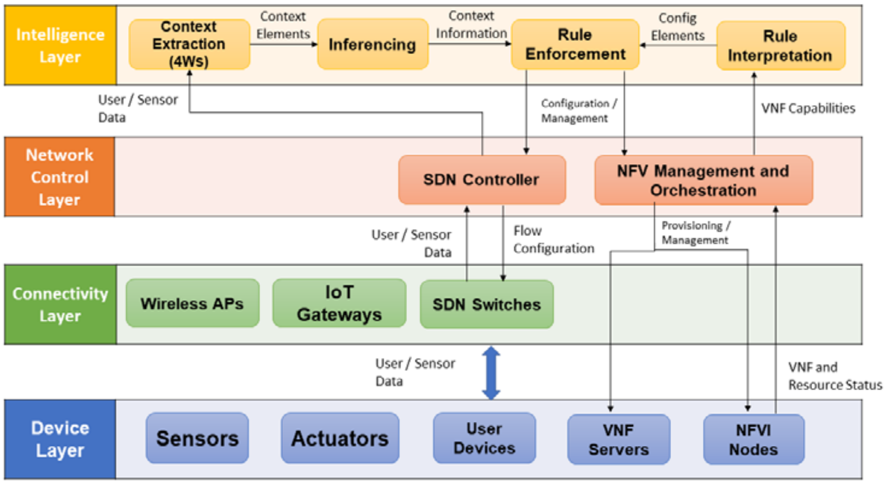

Fig. 3 Proposed Context-Aware IoT Framework

requirements vary depending on the context of the communicating endpoints and the nature of the data being transmitted, it is expected that the flow tables entries will also be regularly changed using the southbound API of the SDN controller to control the forwarding behavior of SDN switches.

D. Intelligence Layer

The intelligence layer must include the building blocks for the processing of context information from data traffic and from them, determine the appropriate security functions to deploy and apply on traffic. To do so, it must include a rule interpretation module that can take user-defined security policies for various application states and translate these into identifiers and configurations intended for security devices or functions available in the network.

A module for context extraction takes information from packets for later inferencing. These can include packet header and application payload content. Depending on the nature of the application, these raw data taken from packets may be further interpreted and aggregated to form composite context-related information. These may be fed to an inferencing module so that full context from a packet or multiple packets may be determined. The actual implementation is likely to vary significantly among different applications. This can use rule-based approaches, statistical approaches, or machine learning models. Reliance on previous states to determine context also can be required. Once context is determined, a rule enforcement module can match the context with the appropriate security polices and configurations from rule interpretation so that it directs the SDN controller and NFV Management and Orchestration entities in the network control layer to deploy VNFs and adjust traffic.

VI. Use Cases

The application of such framework in a real-world scenario may be illustrated by the following use cases.

A. Building monitoring

Building monitoring systems typically control the building and individual unit heating and ventilation, water supply, electrical supply, sprinkler system, lighting, entryways and more. Several of these aspects have a direct impact on occupant safety; and access to collected data and authority to change operating parameters must be strictly controlled. Without security measures, a malicious user may gain access to these critical building controls to waste resources or compromise the physical security of building occupants.

Given these, access can be controlled based on the role of the user, such as management, tenant, contractor or guest; the sensor or actuator to be accessed; its location and ownership, such as in tenant's unit, common area, or outside the building; time of day; nature of data being collected or configured; and possibly, prior events as well. For example, a maintenance contractor may be granted access to devices inside a tenant's unit during work hours only if the tenant is present inside, the device is currently on its regular maintenance schedule or a prior malfunction report was lodges on the system. Possible network functions could be AAA servers for user authentication and firewalls that restrict access to device management interfaces, functions, and allowable settings.

B. Healthcare

The IoT finds its use in healthcare in the form of patient monitoring systems and assistive technologies. The term Internet of Medical Things (IoMT) was coined with the proliferation of wearables that measure various biological signals such as heart rate, blood oxygen levels, sleep patterns, and more, as well as record user location in relation to their physical activity. As these are highly associated with personal information, privacy is highly significant in this area.

Healthcare applications likely need to control access to data depending on user – owner, personal doctor, general healthcare professional, etc.; device, and type of data. As an example, the owner of a fitness tracker can be allowed to freely access records of routes used for a daily jog; but this information can be deemed irrelevant to the user's personal doctor and hence should not be made accessible. Similarly, due to the personal information involved, there can be a need to use confidentiality and integrity-preserving mechanisms depending on the sensitivity of the transmitted data. For instance, a patient whose vitals are monitored and transmitted to a remote medical facility due to an underlying condition needs this data to be secured to avoid exposure that can reveal sensitive personal health information. Network functions that can be supported in this application include AAA servers, firewalls, encryption key servers and VPN gateways that are provisioned as needed if sensitive data needs to be transmitted.

VII. Conclusion and Future Work

In conclusion, this paper emphasizes the importance of considering contextual elements when applying security measures in an IoT application. A 'one-solution-fits-all' static design for the security of an IoT application is not robust and flexible enough to address the requirements for security due to the dynamic, heterogeneous and context-rich nature of an IoT application. To address this, a solution that is equally dynamic is needed. A framework that harnesses the flexibility of SDN and NFV is proposed so that security functions can be deployed and network traffic can be rerouted to and from security functions as needed according to policies based on the context of ongoing communications in an IoT application.

For future work, the functional elements of the framework will be implemented and deployed in the suggested use cases to test the performance and suitability of the design in real-world scenario.

References

[1] J. Bradley, J. Barbier and D. Handler, "Embracing the Internet of Everything to capture your Share of $14.4 trillion," 2013.

[2] IEEE, "Towards a definition of the IoT," 2015. [Online]. Available: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. [Accessed 15 June 2016].

[3] ITU, "Y.2060: Overview of the Internet of Things," 2012. [Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I. [Accessed 16 June 2016].

[4] J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, February 2014.

[5] D. Freemantle, "A referencearchitecture for the Internet of Things," WSO2, 2015.

[6] J. Granjal, E. Monteiro and J. Sa Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," IEEE Comms. Surveys & Tutorials, vol. 17, no. 3, pp. 1294 - 1312, 2015.

[7] P. Porambage, et al, "The quest for privacy in the Internet of Things," IEEE Cloud Computing, vol. 3, no. 2, pp. 36 - 45, 2016.

[8] A. Molina Zarca, et al, "Security management architecture for NFV/SDN-aware IoT systems," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8005-8020, 2019.

[9] M. B. Yassein, Q. Abuein and S. A. Alasal, "Combining software-defined networking with Internet of Things: Survey on security and performance aspects," in 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, 2017.

[10] P. Martinez-Julia and J. Skarmeta, "Empowering the Internet of Things using software defined networking," IoT6.

[11] T. Murakami and A. Fujinuma, "Ubiquitous computing: Towards a new paradigm," Nomura Institute, 2000.

[12] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, 2018.

[13] S. Kraijiak and P. Tuwanut, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," in 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), Shanghai, 2015.

[14] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 0250-10276, 2020.

[15] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347 - 2376, 2015.

[16] S. Symanovich, "The future of IoT: 10 predictions about the Internet of Things," NortonLifeLock Inc, 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. [Accessed 11 April 2021].

[17] E. de Matos, R. Tiburski, L. Amaral and F. Hessel, "Providing context-aware security for IoT environments through context sharing feature," in 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, 2018.

[18] N. Ghosh, S. Chandra, V. Sachidananda and Y. Elovici, "SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT," EEE Internet of Things Journal, vol. 6, no. 6, pp. 10773-10785, 2019.

[19] P. Brézillon and G. Mostefaoui, "Context-based security policies: A new modeling approach," in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, USA, 2004.

[20] T. Gu, et al, "IoTGaze: IoT security enforcement via wireless context analysis," in IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 2020.

[21] B. Han, V. Gopalakrishnan, L. Ji and S. Lee, "Network function virtualization: challenges and opportunities for innovations," IEEE Communications Magazine, vol. 53, no. 2, pp. 90-97, 2015.

[22] ETSI, "Network functions virtualisation (NFV) architectural framework," European Telecommunications Standards Institute, 2013.

[23] Festijo, E., Jung, Y., and Peradilla, M. "Software-defined security controller-based group management and end-to-end security management," Journal of Ambient Intelligence and Humanized Computing, vol. 155, pp. 89-96, 2019.

[24] D. Kreutz, et al, "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, 2015.

[25] Jung, Y., Peradilla, M., and Agulto, R. "Software-defined security controller-based end-to-end packet key security management," Procedia Computer Science, vol. 10, no. 9, pp. 3365-3382, 2018.

[26] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable network," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617-1634, 2014.

[27] M. Mitchiner and R. Prasad, "Software - defined networking and network programmability: Use cases for defense and intelligence communities," January 2014. [Online]. Available: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/software_defined_networking.pdf. [Accessed 18 August 2016].

[28] H. Huang, J. Zhu and L. Zhang, "An SDN-based management framework for IoT devices," in 25th IET Irish Signals & Systems Conference (ISSC 2014), Limerick, 2014.

[29] M. M. Mazhar, et al, "Conceptualization of software defined network layers over Internet of Things for future smart cities applications," in 2015 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Orlando, FL, 2015.