International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I12P102

Volume 69 Issue 12, 5-9, December 2021


*Original Article*

# IoE Security through Multi-Agent SDN

Kumar D[1], C. Veni[2]

[1]*Research Scholar, Department of Computer Science, VLB Janakiammal College of Arts and Science, Coimbatore, India.*
[2]*Assistant Professor, Department of Computer Science, VLB Janakiammal College of Arts and Science, Coimbatore, India.*

Received Date: 08 November 2021
Revised Date: 10 December 2021
Accepted Date: 21 December 2021

***Abstract -*** *The IoE is an intelligent connection of people, processes, data, and things (IoT). Thus IoE combines the converged networking/infrastructure with the process such as automation/orchestration and data science/analytics altogether for effective use by the people. IoE data is very vast and complicated, which could make available real instance environment and reactive information concerning such real things with reference to the environment. In order to retrieve significant and useful information from this massive IoE data, efficient frameworks are required which can be able to analyze the data satisfactorily. Therefore, advanced techniques are required for analyzing real-time, highly scalable data generated by IoT devices and enhancing security in the IoE environment. The SDN agent in a multi-agent environment can implement edge node-specific security and data transfer policies that are framed specially for each IoT cluster of network devices. The proposed framework entitles agent-based modeling with SDN to provide enhanced security and automation. The data may even pass through multiple agents for different purposes with the cognitive orchestration mechanism to transfer data packets to the respective endpoint like cloud service or any other data plane.*

***Keywords -*** *IoE, Internet of Everything, Security, SDN, Multi-agent.*

## I. INTRODUCTION

The recent advancements in networking have introduced a wide variety of concepts that are integrated with other fields of Electronics and communication. Some of such concepts are Cloud-based computing with VPC and cluster shared volume, Software Defined Networking, Network Function Virtualization, Virtual LAN, grid computing, edge computing, osmotic computing, intent-based networking, and so on. The networking in these ways is highly automated and orchestrated with software-defined virtual policies. By evolution and improvement of such a wide variety of advanced networking models, the performance along with security and QoS are given high importance on one side, and the implementation complexity, as well as maintenance cost, is expected to be reduced drastically at the other side.

Internet of Things (IoT)[2] is an abbreviated term to denote devices as things or objects which are used to collect and transfer data over the Internet for a particular purpose or use case without human intervention. IoT is usually considered to workout with electronic devices that have very limited memory and processing power. The Industrial IoT (IIoT) is another segment with large-scale IoT usage such as millions of IoT devices for a particular use case such as farming, healthcare, weather monitoring, urban planning / smart cities, and so on. For example, crowdsensing is a term used to collect a large amount of data[1] from a variety of sensing devices geographically grouped to provide useful information about particular needs such as vehicle traffic management in urban/metro roads and so on. Edge-based cloud computing plays a major role in such IoT-based applications to process large data in real-time analytics and for both automated triggers as well as visualization of data. Also, this convergence the different pillars of Information Technology (IT) and Operational Technology (OT) for smart Industrial usage & transformation.

## II. INTERNET OF EVERYTHING

Internet of Everything (IoE)[3] is a term coined by Cisco Systems, Inc. to the extent of a superset of IoT in machine communication encompassing the data analytics, people/humans, and processes involved. According to Cisco, the IoE is an intelligent connection of people, processes, data, and things (IoT). IoE on the broad-scale covers P2P (Person to Person), which is part of the people connected to the internet, M2M (Machine to Machine) with IoT as its subset, P2M / M2P (Person to Machine) like Smart Home / Office automation setup. This is also indicated in Fig. 1 with the relevant technologies involved, such as Big Data and Cloud. The P2P internet-based communication as a decentralized model has a wider multi-dimensional scope which has evolved for decades. But P2M / M2P being a human-machine interaction, needs stateful cognitive experiences, which is part of the ongoing and future trend of co-working model between humans and machines considered to be the next generation technological revolution, mainly driven as an evolution of all the IoE elements. The IoE architectural process overview with all its interconnected four elements and services is as shown in Fig. 1 below.

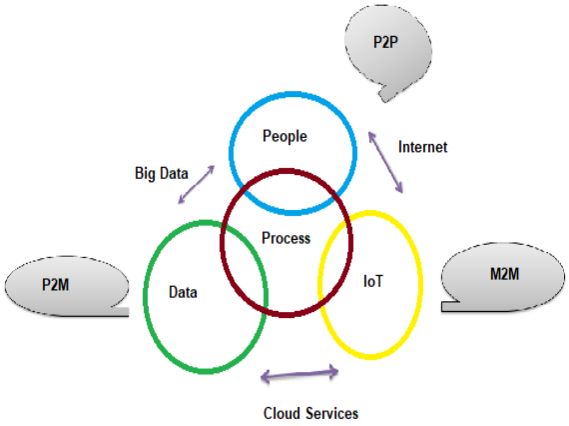


**Fig. 1 IoE Elements Overview**

The IoE is an integration of various elements to provide an expected unique solution. As shown in Fig. 1 above, the IoE involves the interconnection of its 4 elements with other technologies like cloud services to provide a pervasive automation process that can handle a huge amount of streamed data. Artificial Intelligence can be applied in each of these elements to provide cognitive solutions. The IoE involves both data from IoT devices and humans/people. IoT data could be from any source, like an embedded object connected with sensors with no verification for originality. Hence, IoE security is a union of protection of data as well as privacy issues with appropriate legal standards applied. The data security in IoE involves life cycle management with a series of steps in a cyclic manner. The steps include data generation, transmission, grouping, collection, storage, analytics, and so on.

## III. IOE SECURITY THROUGH SDN APPROACH

SDN[4] is a software-based approach; it can provide a reliable and high-performance network with security in-built and applied across the architecture and delivered as a service to protect the security Triads (Confidentiality, Integrity, and Availability). As it is more of a security configuration, the best practices and policy implementation through various procedures can be applied easily and quickly to specific targets/abstraction layers or the network as a whole. Also, SDN can handle anomalies in various effective ways quickly and effectively. Similarly, detection of malicious behavior and isolation of defective components can be effectively automated with SDN security policies[5][6]. According to Gartner[7][8], SDN and cloud computing can provide improved security measures. The following security measures are considered vital for SDN.

- Effective IAM (Identity Access Management)
- Configuration compliance
- Strong security parameter for interfaces
- Automated incident and event management with orchestration
- Access rule policy enforcement
- Visibility services
- Threat analytics
- Backup and redundancy

But the main threat in SDN security is the possibility of the SDN controller itself being compromised. It is a single point of failure, which needs extreme safeguard measures from any security attack. Following are some of the common vulnerabilities identified in SDN irrespective of application/domain-specific factors.

- Application-based issues
- API based issues
- Zero-day vulnerabilities
- Spoofing and poisoning based attack
- DDoS attack

The security threats may also vary according to the type of attack, sensitivity, and layer that is compromised.

## IV. MULTI-AGENT (MA) BASED SDN

In SDN, agents form the main part in each of the layers, which could be applied to multiple segments with goal-directed behavior such as coordination, prioritization, policy enforcement, data traffic management, and so on. MA is composed of multiple interacting agents that perform actions in a complex environment, which may be difficult for monolithic agents. Such an environment could be virtual, continuous, or discrete with cognitive procedures and highly fault-tolerant. The agent performs different functions such as coordination, policy enforcement, updates, event triggers, traffic management, elasticity, and so on. The agent also updates on the progress/status to the controller. The trust domain as management functionality is applied with MA to segregate the logical extension within the domain. Similarly, a hybrid environment could also be applied with MA-based SDN to support the sharing of virtual resources with partial control by the SDN controller. This involves different levels of abstraction and function sets as X and Y-axis in a graph respectively for each trust domain or SDN coordinators. By this, different network policies could be easily instantiated in real-time by respective isolated SDN controllers with various depth, elasticity, functions, and interactions. This approach is a boon for cloud-based IoE networking to reduce region-based dependency and maximize the efficacy of shared resources. Cloud networks with software virtualization frameworks could instantiate multi-tenancy features to drive several applications as part of the same infrastructure. Such cloud adoption of software virtualization framework could improve the network scalability in a respective cloud environment for both the infrastructure as well as big data-related issues.

## V. EXISTING SDN AGENT-BASED APPROACHES

Alexandre Passito et al.[9] have proposed a framework named Agent for Network OS (AgNoS), in which agents are used to handling a network domain in an SDN network. The SDN agents are also responsible for modeling various objects in a network such as the services, protocols, routing mechanism, network access control list, and also users. The agents coordinate to control the complete network by sharing information regarding their specific tasks related to the domain model. The agents are orchestrated and controlled by the SDN controller, which controls the process flow and directs the tasks of the agents with required information about process flow, autonomy, and dependencies. As a research work, the researcher has used Mininet to simulate the DDoS attack scenarios and illustrate the potential of their framework in mitigating such attacks.

Further, similar to the AgNos framework for agent-based security in SDN-based networking, Kuklinski et al.[10] has provided additional management nodes as a partition in the SDN network such that by the partition of a big network into various classification, these additional nodes are used to control each of the different domains by available agents assigned within the network with specific network management tasks to each of the agent. This framework, according to the researcher, could reduce the overloading of the SDN controller and provide better control in network management.

Similarly, L. Ochoa Aday et al.[11] had put forward an SDN agent-based topology discovery technique to effectively discover network topology wherein the SDN controller is used to orchestrate multiple agents in the network, with each of the agents to implement the software distributed topology discovery protocol (SD-TDP). This protocol is used to discover a delay confined shortest path tree from the controller to the network and its agent. This proposed technique organizes the network topology information in an aggregated manner before being sent to the SDN controller.

Sharma V[12] introduces MAS-based intrusion detection and recovery architecture which can be incorporated to prevent and alleviate real-time security attacks such as addressing the DDoS attacks in SDN networks. The proposed solution is deployed at the SDN controller to maintain information about different network events such as the flow table, network policies, topology, etc., and further, detect and mitigate security threats through its available knowledge base and policy-based reasoning. It consists of various other built-in features such as agent-based monitoring, knowledge domain, and interface engine.

Similarly, to deal with the various security issues in SDN, Garc´ıa-Marino, et al.[13] presents an agent-based trust and reputation simulator which can provide the trust reputation of each network element. With a defined trust model in place, the solution is used to test the trust policy of the network and its components, including controllers, agents, devices, and other isolated protocols. This solution uses an agent-based approach to have three types of agents, viz. the network agent represents the network devices/components, the SDN controller is embodied as controller agent, which also represents the isolated protocols, and other agents represent malicious behavior as malware. The trustworthiness of each agent is checked by sending the random data packet to each agent and then evaluating the findings with its trust model. IoE environment involves both infrastructure and data analytics that may involve real-time processing, which needs the flexibility provided by SDN-based cloud services. A variety of security threats prevail in SDN implementation and usage, which need to be addressed in effective ways. The big geo-spatial data and cloud integrations can be implemented for more flexibility, elasticity, improved performance, and security.

## VI. CHALLENGES

Along with the various challenges that the current approaches are undergoing, two major parts of concern are effectively handing out the IoT data with improved security while it is in transit from IoT devices to the public cloud. In the above research review, the main focus is on accumulating and handling non-spatial IoT data, whereas the issues regarding handling and securing through spatial integrated IoE data are sidelined. Innovative IoE data processing techniques are required at different application/network nodes to label and handle such unleashed data. Therefore, advanced techniques are required for analyzing real-time, highly scalable data generated by IoT[14] devices and enhancing security in the IoE environment.

## VII. PROPOSED SOLUTION

The rapid evolution of cloud services and the Internet of Everything (IoE) has led to drastic data overhead with millions of connections used in real-time analytics together with multiple cloud services leading to exponential congestion than the traditional networks[15]. Hence, it is essential to redefine the cloud services usage with different topologies such as Edge computing, Fog computing[16], Osmotic computing, and so on. Edge computing is a decentralized computing technique to denote the cloud services available at/near the origination of data rather than at the cloud data center, by which the data traffic to the data center is reduced to a large extent leading to better bandwidth, lower latency; and quick response to real-time analytics[17] such as IoE. The data is filtered by edge computing to decide whether to respond back or send the data to the cloud based on certain parameters. Hence, it is also considered as an intermediate layer/node between the data publisher and the cloud network. The proposed system could provide both improved performance and security through efficient traffic engineering with additional security parameters as part of the configuration by the SDN controller

in the network flow with cognitive and simplified routing mechanisms applied to such SDN agents with other processes as detailed below.

## VIII. COGNITIVE ORCHESTRATION MECHANISM IN SDN

Cognitive Orchestration is a mechanism applied through smart capabilities such as Edge-based computation and so on. The Edge based computation is a distributed computing paradigm to improve latency-based issues in processing a huge amount of data as well as providing the same cloud-based cognitive services and content caching to the local IoE environment grid in a decentralized manner with improved scalability, efficiency, throughput, and security with privacy. This approach reduced the high volume of data transfer in the SDN, the consequent traffic, and thus improved network optimization and efficient use of edge nodes with a different form of preferred network policies customized and orchestrated for each node in terms of processing, caching, scalability, and security[18]. For example, once a network security incident is identified with one edge node may not be applicable for other edge nodes due to customized policy orchestration, and hence malicious behavior cannot comprise the whole network with the same simple approach[19]. Fig. 2 below shows the edge node-based agent performance in SDN for improving security-related factors from IoT clusters.

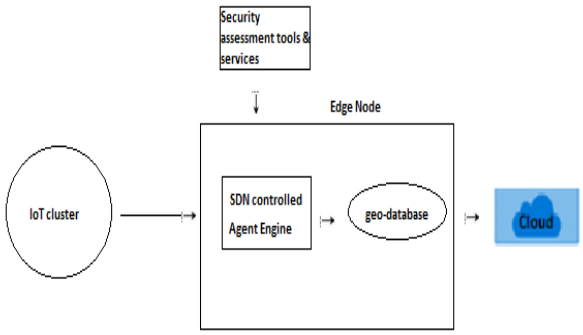


**Fig. 2 SDN Agent in IoT Edge node**

As shown in Fig. 2 above, the IoT cluster with networked devices for various use cases could network with the nearest edge node for processing of data with both security issues as well as streaming to the cloud for further processing after the geo-tagging process from the information available in integrated Geo-database[20]. The agent controlled by the SDN controller can implement edge node-specific security and data transfer policies that are framed specially for this IoT cluster of network devices. The data may even pass through multiple agents for different purposes. The agent herewith is provided with the cognitive orchestration mechanism to transfer geo-tagged data packets to the respective endpoint like cloud service or any other data plane. It may also go for decomposition or data enrichment before such transfer based on the orchestration policies. The data can be indexed, encrypted, structured, and cached based on the configuration parameters set by the SDN controller as part of this cognitive orchestration. It also provides tag-based deletion of your data from both the edge nodes and cloud for easy mass removal of big data as per the data retention policies by the respective data owner through their respective SDN agent. This enhances both the security and privacy factors to a large extent. Another noted functionality is the time-based event trigger of various agent tasks in the edge node for both security and QoS services remotely configured by the SDN controller. This time-based profile goes with the frequency of specific time intervals as well as event-based triggers to process respective data profiles by the SDN agent from IoT cluster data to undergo any of the aforesaid transformations and further processing.

## IX. CONCLUSION

The SDN framework model proposed improves the IoE edge-based control with enhanced security measures by Cognitive routing to multiple agent-based approaches in the SDN architecture. The SDN agent in a multi-agent environment can implement edge node-specific security and data transfer policies that are framed specially for each IoT cluster of network devices. The data may even pass through multiple agents for different purposes with the cognitive orchestration mechanism to transfer data packets to the respective endpoint like cloud service or any other data plane.

## REFERENCES

[1] Akdogan, S. Indrakanti, U. Demiryurek, and C. Shahabi, Cost-efficient partitioning of spatial data on the cloud, 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, (2015) 501-506.
[2] The Internet of Things (IoT) – essential IoT business guide (n.d), retrieved from https://www.i-scoop.eu/internet-of-things-guide/
[3] IOE (n.d), retrieved from http://www.gartner.com/newsroom/id/3598917.
[4] Surendiran,R., and Alagarsamy,K., Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption. SSRG International Journal of Engineering Trends and Technology (IJETT), 4(5) (2013) 2217-2224.
[5] SDN Architecture (2014), retrieved from https://opennetworking.org/wpcontent/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf
[6] A. Akhunzada, A. Gani, N. B. Anuar, A. Abdelaziz, M. K. Khan, A. Hayat, and S. U. Khan, Secure and dependable software-defined networks, Journal of Network and Computer Applications, 61 (2016) 199–221.
[7] A. Akhunzada and M. K. Khan, Toward secure software-defined vehicular networks: Taxonomy, requirements, and open issues, IEEE Communications Magazine, 55(7) (2017) 110–118.
[8] Gartner‘s hype cycle special report for, (2011). Gartner Inc., 2012. http://www.gartner.com/technology/research/hype-cycles/
[9] A. Lapkin, Hype cycle for big data, retrieved from http://www.gartner.com/document/2100215, (2012).
[10] A. Passito, E. Mota, R. Bennesby, and P. Fonseca, Agnos: A framework for autonomous control of software-defined networks, in 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, (2014) 405–412. IEEE.
[11] S. Kuklinski, Programmable management framework for evolved sdn, in 2014 IEEE Network Operations and Management Symposium (NOMS) (2014) 1–8. IEEE.

[12] L. Ochoa-Aday, C. Cervello-Pastor, and A. Fern ´ and-Fern ´ Mendez, A distributed ´algorithm for topology discovery in software-defined networks, in International Conference on Practical Applications of Agents and Multi-Agent Systems, (2016) 363–367. Springer.

[13] V. Sharma, Multi-agent based intrusion prevention and mitigation architecture for software-defined networks, in 2017 International Conference on Information and Communication Technology Convergence (ICTC), (2017) 686–692, IEEE.

[14] I. Garc´ıa-Magarino and R. Lacuesta, Abs-trusts: An agent-based simulator of trust strategies in software-defined networks, Security and Communication Networks, 2017 (2017).

[15] Khan, Sahrish & Shah, Munam & Khan, Omair & Ahmed, Abdul. Software-Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead. 1-8 (2017). 10.1145/3102304.3102319.

[16] Mervat Abu-Elkheir, Mohammad Hayajneh, and Najah Abu Ali, Data Management for the Internet of Things: Design Primitives and Solution‖, Sensors, (2013) 15582-15612.

[17] Q. Shafi, A. Basit, S. Qaisar, A. Koay, and I. Welch, Fog-assisted SDN controlled framework for enduring anomaly detection in an iot network, IEEE Access, 6 (2018) 73713–73723.

[18] A. Pektas¸ and T. Acarman, Deep learning to detect botnet via network flow summaries, Neural Computing and Applications, 31(11) (2019) 8021–8033.

[19] Bera. Samaresh, Mishra. Sudip, Roy. Sanku Kumar and Obaidat. Mohammad S., Soft-WSN: Software-Defined WSN Management System for IoT Applications, IEEE Systems Journal, 12(3) (2018) 2074–2081.

[20] D. Zhang, F. R. Yu, and R. Yang, A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management, in 2018 IEEE Global Communications Conference (GLOBECOM), (2018) 1-6

[21] Jae Gil Lee, Minseo Kang, ―Geospatial Big Data: Challenges and Opportunities‖, Journal of Big Data Research, 2(2) (2015) 74-81.