ENHANCED IoE SECURITY BY GEO-TAGGED AGENT BASED SDN

KUMAR D[1] and Mrs. C. VENI[2]

[1]Research Scholar, Department of Computer Science,
VLB Janakiammal College of Arts and Science, Coimbatore-641042, TN, India
[2]Assistant Professor, Department of Computer Science,
VLB Janakiammal College of Arts and Science, Coimbatore-641042, TN, India

ABSTRACT

The IoE (Internet of Everything) is rapidly evolving across all segments but subsequently introducing several new challenges in terms of processing IoT generated data, privacy, performance, resilience, network QoS, security and operational assurance. In order to retrieve meaningful information from this massive IoE data, efficient frameworks is required which can be able to analyze the data satisfactorily. SDN (Software Defined Networking) as a software oriented approach with Virtual Network Functions (VNF) provide controlled traffic engineering of IP packets in various ways with improved performance and policy oriented enhanced security. Geo-tagging is the process of appending geographically identifiable spatial metadata to a particular relevant object so that the object could give more relevant self-reliant information on itself. The geo-tagging being a flexible methodology in SDN approach to handle security provides improved handling of IoE data based on the ecosystem applied. In this research, it is proposed for an SDN enabled control plane based orchestration that leverages geo-tagged agent based architecture to combat malicious IoT nodes in the IoE process to enhance its security.

Keywords: *IoE security, SDN, geo-tagged agent*

1. INTRODUCTION

Internet of Things (IoT) is an abbreviated term to denote devices as things or objects which are used to collect and transfer data over Internet for a particular purpose or use case without human intervention. Such data transfer can be used to interconnect objects for further processing, client-server mode for data storage, information processing for human action, sensing to a transducer or actuation and any other such mechanisms. IoT is usually considered to workout with electronic devices that have very limited memory and processing power. Some of the most common IoT use cases are Smart Home / Office, Smart Wearable, etc [1]. Some of the common IoT sensors are proximity sensors, RFID sensors, light sensors, etc. The common protocols used in IoT include NFC, RFID, Bluetooth, etc. IoT is majorly categorized as short-range, medium-range and long-range wireless based on the protocol used in the data transfer between IoT objects. IoT along with other trending technologies such as Big Data, cloud based edge computing, Machine Learning, digital twin, mixed reality, etc are expected to lead the future smart Industrial revolution towards the Automation age.

Internet of Everything (IoE) is a term coined by Cisco Systems, Inc. to extent as a superset of IoT in the machine to machine communication encompassing the data analytics, people / human and processes involved. According to Cisco, the IoE is an intelligent connection of people, process, data and things (IoT). Thus IoE combines the converged networking / infrastructure with process such as automation / orchestration and data science / analytics altogether for effective use by the people. This capability of IoE can provide real-time data analytics with enormous amount of data connecting millions of IoT devices in an automated and people-oriented process integrated with edge based cloud services [2]. The Smart City implementation like automated urban traffic management with self-driving vehicles and integrated Smart grid electricity power flow is a relevant example of IoE significance in future technological landscape [3]. Since TTL (Time to Live) with semantic modelling and relevant notifications play significant role in IoT landscape, it can be efficiently managed through IoE integration.

2. SDN & IoE

SDN architecture [4] is flexible, agile and elastic to handle large volume of data (Big data) [5] in its distinguished data layer with QoS which is essential for IoE. IoE as grouping of IoT devices and their data within the network; SDNs dynamic configuration supports the network scalability as well as the heterogeneous environment. A typical SDN integrated IoT schematic view with layers is given in figure 1 below.

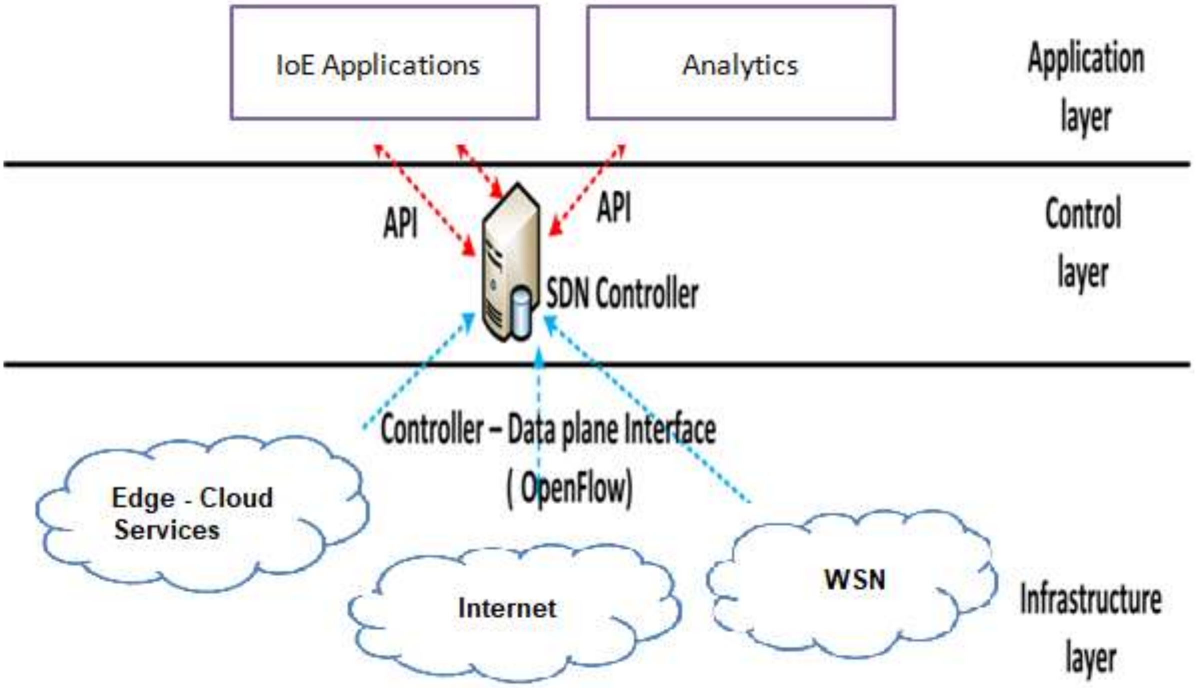

Figure 1 – SDN integrated IoE schematic view

As shown in figure 1 above, the applications in application layer interact with the heterogeneous IoT environment in data / infrastructure layer through APIs as part of the SDN and controlled by the SDN controller. This could be applied to both wired and wireless network environment. All security and network traffic control could be applied instantly with the respective applications in application layer. Bera et al. (2018) [6] has proposed a modified SDN in wireless IoT network for real time application aware service provisioning, specifically to the WSN (Wireless Sensor Networks), which is considered as the backbone for IoT based projects like self-driving vehicles, urban vehicle traffic management and so on. Similarly, Khan et al. (2017) [7] discuss the suitability of IoT networking with SDN. SDN can play a vital role in management of heterogeneous network by eliminating difficulties related to configuration, resource allocation, inter communication and so on. The load balancing efficacy as part of traffic engineering, layer decoupling, interface API and resource management among these architectural frameworks are analysed.

Geo-tagging is the process of appending geographically identifiable spatial metadata to a particular relevant object so that the object could give more relevant self-reliant information on itself. It usually contains longitude and latitude coordinates, altitude, bearing, accuracy, geographical place information, distance, time stamp, etc. to denote the relationship with the tagged object in a location specific manner. The geo-tagging being a spatial-temporal data, increases the data size with heterogeneity and is dynamic. L. Chen et al. [8], [9] emphasized a technique for integrating two R-trees, for mass insertions of geo-spatial data. In this solution, initially small trees are constructed and then it further attempts to locate whether the proper access point is available in the large tree, where the respective small trees roots are available. The overflow is handled (if needed), through Z - curve by implementing partitions and local index by separate insertion method.

Similarly, K. Wang et al. [10] proposed a simple Spatial Data Parallel Processing Framework (SDPPF) for large scale calculation and parallel processing of spatial data with faster processing as well as handling large volumes effectively. Also in line, for big geo-spatial data handling, B. Wang et al. [11] put forward the geometrically searchable encryption (FastGeo) methodology, which can be used to index geospatial data in to hash table and thereby reduce the time required to search.

GIS provides special characteristics coding to integrate with the geo-data objects called '*Geo-tagging'* for various purposes. Geo-tagging is a geo-spatial data as meta-data to provide additional geo-graphic information about the object which is tagged to the object data. For example, a photo shared with location as geo-tag among particular users in a social networking site provides the location and other related details about the given picture to the viewers for better clarity even after long duration. Geo-tagging uses metadata to provide historical tracking of objects effectively in real-time with all manipulations and transfer recorded in due course. It is considered an effective monitoring and tracking mechanism in various use cases like E-Governance, Urban Planning, effective network infrastructure implementation and so on The meta-data provides additional information like coordinates involving longitude and latitude, elevation data indicating the irregular surface of Earth with gravity and sea level altitude and such other information tagged to the relevant data. ISO 19115 standard is the most widely used one for geo-spatial meta-data. The meta-data can be stored, processed and used by applications in various formats like XML, JSON and so on for different kinds of heterogeneous and distributed environments.

3. PROBLEM STATEMENT

IoE is generating enormous amount of streamed, structured & unstructured, real-time big data. Researchers emphasise in different ways to design novel frameworks to retrieve more significant information from these increasing data volumes. Pioneering IoE data processing methods are essential for handling these unleashed data. 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 with this massive IoE data, efficient frameworks are required which could be able to analyze the data satisfactorily in real-time. Therefore, advanced techniques are required for analyzing real time highly scalable data generated by IoT devices and enhance security in the IoE environment through efficient geo-based tracking mechanisms.

4. PROPOSED SOLUTION

SDN (Software Defined Networking) as a software oriented approach with Virtual Network Functions (VNF) provide controlled traffic engineering of IP packets in various ways. The literature review shows different research gaps [12] - [18] that have left behind while processing IoE geo spatial data, in parallel, efficient and secure. Hence, the SDN system thus developed tags all elements of IoE viz. the data and devices as geo-tagged to the respective agent in SDN. Similar to the different geo-tag framework described above in literature review, the geo-tag with the agent provides the non-repudiation and originality sequence of the data flow with the IoE environment, including multiple IoT nodes and gateways. This also provides the timestamp, metadata and log history for incident tracing as part of the security incident management through parallel index processing with scalability to process big geospatial data. The importance of this research area is analyzing IoE geo-spatial data in real time for particular events or patterns of interest to enhance security. 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. For this to effect, the geo-spatial indexing with parallel mechanism and multi-agent based traffic engineering integrated with the geo-spatial indexing is applied to the SDN agents with other processes as detailed below.

4.1 GEO-SPATIAL INDEXING OF IoE IN SDN

An effective partition strategy is essential for the performance of parallel indexing with equal load balancing among all the nodes participating in this parallel processing. The quality of performance is directly proportional with such data oriented partition technique involved in the parallel processing of big data streamed in the IOE Environment. The stream processing involves tasks of map and reduce mechanism to real time analysis with caching for easy retrieval of certain queries handled often and reduced latency with replicas. This mechanism provides dynamic load balancing between parallel nodes with high throughput, low latency and eventually parallel processing of streamed data.

The R-tree parallel mechanism for geo-spatial big data indexing with streamed data processing engine like Apache Spark with cluster form of computing the data nodes has high memory utilization with less execution time. This mechanism provides improved performance and throughput for IoE based data processing of streamed data compared to the sequential processing by other mechanisms. Also, the index may also be constituted as ‘secured’ index which is an encrypted indexing of the corresponding identifier data along with geo-tag parameters for enhanced data security for sensitive information. In such context, there exists an ‘encrypted’ query to deal with the search phase of secured index to obtain information back to the users. There could be slight latency issues, if encrypted query is used across huge amount of secured index data compared to the normal process. Hence, the network policies of defining sensitive data for encrypted index should be well optimised in pair with the QoS requirements. Efficient parallel processing of encrypted query among different nodes by cognitive mechanisms proposed below could solve latency issues to great extent with more flexibility and efficiency.

4.2 GEO-TAGGED AGENT TRAFFIC ENGINEERING IN SDN

The geo-tagged agents in SDN provide multiple to multiple mapping between the objects and agents within the SDN. Each agent incorporates a geo-tag within itself to support the data transfer through / within SDN network such that the routing and handling of such data can be tracked through such geo-tag encompassed with the data packet. This meta-data thereby supports the tracking, monitoring, event alerts, triggers, security incident handling and so on. The geo-tag is unique to such SDN agent with the respective token and dynamic as the SDN processes such requests, so that, the different node traffic of IoE data can be tracked simultaneously by same mechanism. The orchestration and process flow may differ with each agent as determined by the SDN controller, which may include certain independent tasks as well as collaborative and sequential tasks with other agents involved to achieve the target. Such process flow indicates SDN agent action with both directed tasks as well as conditional tasks based on certain logic to overcome the incidental challenges that occur during the execution process. Similarly, the SDN agent can be indicated of the sensitivity, risk level and threats to act upon accordingly in the handling of tasks between the edge nodes, IoT cluster and other agents in the SDN for effective security and compliance implementation as well as efficient QoS in the network. A typical transfer of data using SDN agent with geo-tag mechanism is shown in figure 2 below.

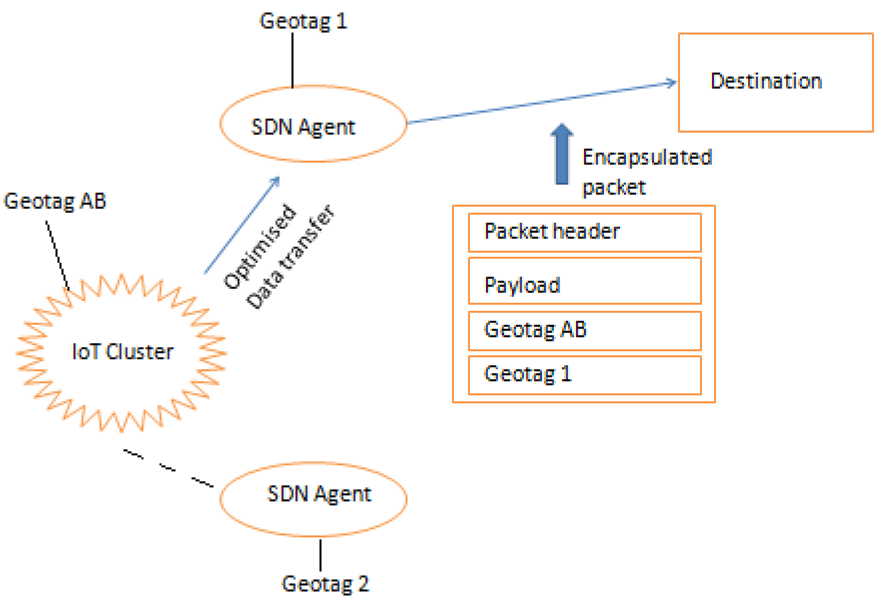

Figure 2 – Geo-tagged agent based data transfer

The traffic engineering involves proposed traffic classification based on above parameters in distributed architecture and process flow of information among the SDN agents in co-ordinated manner with customizations as defined in the orchestration process for each agent. It involves the classification with different parameters such as source, destination, protocol, sensitivity, risk level, agent identity with geo-tag, routing, IoT cluster, IoE process and so on. These determine the cognitive routing by the controller and respective agents from the IoT cluster to the SDN through different edge nodes and intermediate agent processing. As shown in figure 2 above, the IoT cluster with networked IoT devices sends data in the optimised path through SDN Agent with 'geotag 1' and hence the encapsulated packet has geo tag of both the IoT cluster and the respective SDN agent as shown. With Distributed Denial of Service (DDoS) attacks considered the most important threat vectors in SDN, the SDN controller can easily identify malicious intrusions to the data layer through this and keep track of all data flows effectively. The metadata attributes are dynamic in nature and hence real-time processing can be done effectively with low latency, enhanced security and improved performance [19], [20].

5. RESULTS AND DISCUSSION

The SDN based data monitoring differs from the dataset aggregation for security monitoring. The semantics is also added to provide required relationships in effective manner for improved usability as a single data processing set from multiple joins, groups and filters. Internally, further sequential steps such as profiling, transform, variable creation and ingestion may be involved. Finally, the test accuracy and loss function are the main criteria used in determining the effectiveness of the data modelling being done. The close the fit, it provides better accuracy. The cross-validation provides the highlight of such predictions for improvement in test data to be further applied in real-time analytics at later stage. The given cognitive orchestration process in SDN data modelling discussed above undergoes such validation [21], enrichment and processing of data for reduction in loss function and improvement of accuracy through a cyclic process. The output of the processed data after hyper tuning [22] can be plotted to identify such areas and provide various effective remediation. This could work with both the encrypted and unencrypted data as the geo-tag part of metadata is given preference in the security incident handling than the real data from the nodes. But the performance issues can be identified in handling of such data processing with the type of cryptography used and processed at differed stages although the general data transfer is not affected. The security enhancement can be provided in various ways for the IoE data apart from the encryption methods but still encryption is considered vital for multiple reasons to handle the security of data at rest / transfer.

6. CONCLUSION

The SDN framework model proposed improves the control with enhanced security measures by integration of geo-tagged parameters to different objects part of the SDN architecture. Adding geo-tags with geo-spatial data provides improved networking capabilities, protecting sensitive data transfer through unauthorised medium with geo-fencing features, detecting anomalies in network traffic through effective tracking and monitoring mechanisms and so on. For such effective security monitoring, effective trusted tracking mechanisms such as a geo-tag, self - troubleshooting, event triggers are vital. The framework works as multi-staged process for this geo-tagged agent based SDN viz. Geo-tagging, indexing and processing. The approach proposed and analysed may have limitations with the hardware setup, type of system software used and other network approaches integrated along with.

REFERENCES

[1] The Internet of Things (IoT) – essential IoT business guide (n.d), retrieved from https://www.i-scoop.eu/internet-of-things-guide/

[2] IOE (n.d), retrieved from http://www.gartner.com/newsroom/id/3598917

[3] Mervat Abu-Elkheir , Mohammad Hayajneh and Najah Abu Ali, Data Management for the Internet of Things: Design Primitives and Solution‖, Sensors 2013, 13, 15582-15612

[4] SDN Architecture (2014), retrieved from https://opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf

[5] A. Lapkin, Hype cycle for big data, 2012, retrieved from http://www.gartner.com/document/2100215, Jul. 2012

[6] Bera. Samaresh, Mishra. Sudip, Roy. Sanku Kumar and Obaidat. Mohammad S., "Soft-WSN: Software-Defined WSN Management System for IoT Applications" IEEE Systems Journal, vol. 12, no. 3, pp. 2074–2081, 2018

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

[8] L. Chen, R. Choubey and E. A. Rundensteiner, ―Bulk Insertions into R-trees Using the Small-Tree-Large-Tree Approach,‖ in Proc. ACM GIS, 1998, pp. 161–162

[9] L. Chen, R. Choubey and E. A. Rundensteiner, ―Merging Rtrees: Efficient Strategies for Local Bulk Insertion,‖ GeoInformatica, vol. 6, pp. 7–34, March 2002

[10] K. Wang, J. Han, B. Tu, J. Dai, W. Zhou and X. Song, "Accelerating Spatial Data Processing with MapReduce," 2010 IEEE 16th International Conference on Parallel and Distributed Systems, Shanghai, 2010, pp. 229-236

[11] B. Wang, M. Li and L. Xiong, "FastGeo: Efficient Geometric Range Queries on Encrypted Spatial Data," in IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1

[12] Gartner‗s hype cycle special report for 2011, Gartner Inc., 2012. http://www.gartner.com/technology/research/hype-cycles/

[13] 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, pp. 405–412, IEEE, 2014

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

[15] Jae Gil Lee, Minseo Kang, ―Geospatial Big Data: Challenges and Opportunities‖, Journal of Big Data Research, Volume 2, Issue 2, June 2015, Pages 74-81

[16] 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, vol. 6, pp. 73 713–73 723, 2018

[17] 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), pp. 686–692, IEEE, 2017

[18] A. Akdogan, S. Indrakanti, U. Demiryurek and C. Shahabi, "Cost-efficient partitioning of spatial data on cloud," 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, 2015, pp. 501-506

[19] 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, vol. 61, pp. 199–221, 2016.

[20] A. Akhunzada and M. K. Khan, "Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues," IEEE Communications Magazine, vol. 55, no. 7, pp. 110–118, 2017.

[21] 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, pp. 1-6

[22] A. Pektas¸ and T. Acarman, "Deep learning to detect botnet via network flow summaries," Neural Computing and Applications, vol. 31, no. 11, pp. 8021–8033, 2019.