International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)

Building Scalable Security Configuration Systems for IoT Devices

Laxmana Kumar Bhavandla
Independent Researcher, USA

Article Info
Volume 7, Issue 6
Page Number : 453-458

Publication Issue :
November-December-2021

Article History
Accepted : 15 Dec 2021
Published : 30 Dec 2021

ABSTRACT

The exponential growth of the IoT devices has brought new concerns in terms of security settings across a large population. Due to the multiple interconnected smart devices, differentiation of the operating conditions and active changes in the security threat landscape, solutions for IoT must be scalable and adaptive. This present paper examines the prospects of designing scalable security configuration systems for IoT devices with particular focus on factors such as real time adaptability, automated deployment and control. The essential areas include studying the present issues, assessing the existing paradigms and contributions which recommended emerging approaches relying on cloud based systems and distributed architectures. The results also show that the models put forward do not only improve security resiliency at scale but also simplify compliance with regulations during the development process. In the final part, distinct possibilities of using artificial intelligence and blockchain to enhance IoT security settings are considered to provide practical guidelines for developing a more secure IoT environment.

Keywords : IoT, DDoS, NAC , I, Scalable Security Systems, Real-Time Adaptability, Automated Deployment, Security Threat Landscape, Cloud-Based Systems, Distributed Architectures, Security Resiliency, Regulatory Compliance

Introduction

Internet of Things IoT is now central to contemporary technological developments where multiple billions of devices are connected to increase productivity in several industries. Although, due to spurt in IoT integration, nowadays a number of IoT networks are being set up which pose immense security threats as these devices do not come with strong built in security parameters and are vulnerable to various cyber attacks. One of the prime considerations that need to be kept into consideration while developing the security models is scalability, due to the massive number of smart devices that will be connected to the network. While traditional approaches to compliance and security configuration work in some small to medium scale networks, IoT environments are more subtle and require a more complex approach in terms of heterogeneity of the set and dynamic natures of the environment. In addition, IoT devices feature varied methods with no universally accepted norms of communication, which makes it challenging to integrate structured security

systems. Computer criminality including unauthorized access, data invasion, and DDoS attacks point to the need for configurations of security settings that can be scaled up to safeguard sensitive information and systems integrity. This report studies on scalability in IoT security configuration systems where current solutions are examined, their constraints discussed and an advanced model drawn. In the context of the discussed approach and its major goals with respect to scalability, real time adaptability and compliance with existing and emerging regulations, the report outlines the criteria for the development of robust security systems that would be able to protect IoT environments from the growing threats.

Literature Review

Envisioning Secure and Scalable Network Access Control

According to Shaik *et al.*2017: The Author explains that IoT continues to grow at a fast pace and new challenges appear especially due to the large number of IoT devices and the ability to regulate access in the heterogeneous large scale networks. Analyzing the added value of the current investigations with reference to the NAC approach, this research identifies the crucial shortcomings of classical NAC strategies and contributes a new framework to overcome these problems. To address this challenge and considering the constantly changing architecture of IoT the authors make several suggestions which includes the enhancement of Scalable Architectures, Efficient Lightweight Authentication protocols and Policy Driven enforcement techniques to address the dynamics of IoT. Invariant attributes are dynamic device profiling, context aware access control and machine learning based anomaly detection which improve Network Security. It also looks into possible advantages like extended extensibility in scalability and integrated facility in managing as well as the problem of excessive computation and conflict with current structures. The authors effectively perform bridges to consider two critical research gaps in order to achieve effective NAC solutions for IoT environments that are secure and elastic.

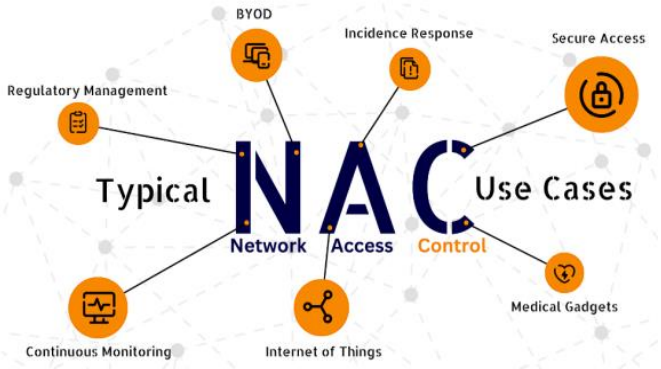

Figure 1: Network Access Control (NAC)

(Source: https://dlabi.org)

A Scalable and Self-Configuring Architecture for Service Discovery in the IoT

According to Cirani *et al.*2014: The Author presents a simple but powerful work that is aiming at creating a self configuring peer to peer (P2P) based architecture that can be used in large scale IoT networks for the purpose of automating the service and resource discovery. Authors also emphasize on availability, stating that addressing it through reducing configuration and maintenance interventions promoted while scale is expected to handle billions of devices. Its approach combines current local and global services discovery techniques based on the Distributed Hash Tables (DHTs) and zero configuration protocols. The architecture allows for smooth local and international communication while promoting the autonomy of both levels. Real world experiment outcomes prove the possibility and efficiency of using the proposed solution. This study emphasizes how the usability of P2P networks advances the IoT fault tolerance, scalability and the availability of resources which are major concerns to IoT implementation. This work undoubtedly helps towards the development of adaptive and self managed IoT service architectures.

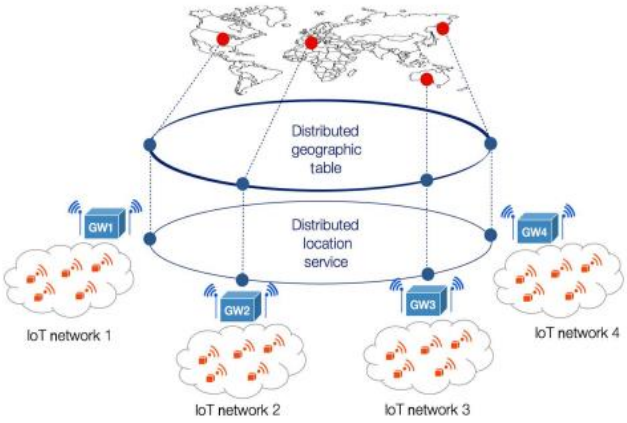

Figure 2: Large scale SD Architecture

(Source: https://inria.hal.science)

Efficient and scalable IoT service delivery on Cloud

According to Li *et al.*2013: It states that a PaaS framework is proposed to avoid the problems associated with vertical solutions that characterized IoT service delivery models that are physically separate. The proposed framework provides for the establishment of the virtual verticals by utilizing the common computing resources and middleware services in the cloud based system. The authors resort to domain mediation as the method to create Caa canonic and domain-specific control applications customized for specific domains, such as building management systems. This solution improves on scalability and maintainability by providing for multi tenant capability and reducing duplicated systems. The implementation comprises event processing data services and context management, to make the appropriate dynamic assignment of the available resources. The presented architecture of the IoT PaaS improves IoT service provision in terms of scaling and flexibility over the various application domains.

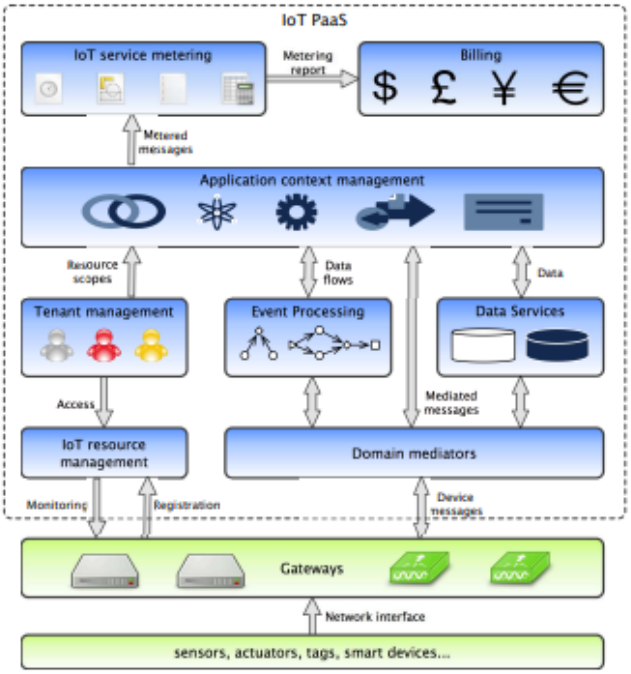

Figure 3: The IoT PaaS Platform

(Source: https://dsg.tuwien.ac.at)

Methods

Data Collection and Processing for Security Logs

Proper security configuration systems always incorporate the process of data accumulation and analysis in order to observe the activity of devices, transgressions of established norms and the risks that they pose. Information gathered has to be from places like devices activity log, Network traffic analysis and system performance which is all about security and operational risk (Noorman *et al.*2017). These logs include both real time and historical data for using a complete set of inputs for analyzing the device behavior under different circumstances. Most important of all, noise filtering, normalization of data values and feature extraction are some of the data preprocessing methods that are vital in data quality and real time analysis. Composite data is analyzed with the help of the data processing technologies with the help of which appearing threats' characteristics are determined. It also comprises auto categorization and ranking of security threats with a view of their potential danger level (Sarkar *et al.*2014). Besides, distributed structures for the purposes of data acquisition are scalable and prevent the latency

problem when analyzing large scale IoT deployments. Taking it further, optimization of the data collection pipeline leads to increased general availability of security configurations.

System Design for Scalability

With regards to scalability and efficiency in configuration of security the proposed system architecture includes cloud based solutions and edge computing. Some devices share a single cloud interface for managing and adjusting security settings as well as for monitoring devices, but logical data processing occurs at edge nodes because the architecture sustains low latency and data usage costs. Software configuration tools and policy compliance engines help organizations to automate the deployment and update of security controls, across the extensive IoT environment (Jiang *et al.*2015). Use of standards that support integration and application programming interfaces allow extension to provide extended compatibility with pre-existing systems flexibility and simplicity of implementation are also arguably improved. This centralized and distributed approach helps maintain the currency of the security configurations in large scale environments.

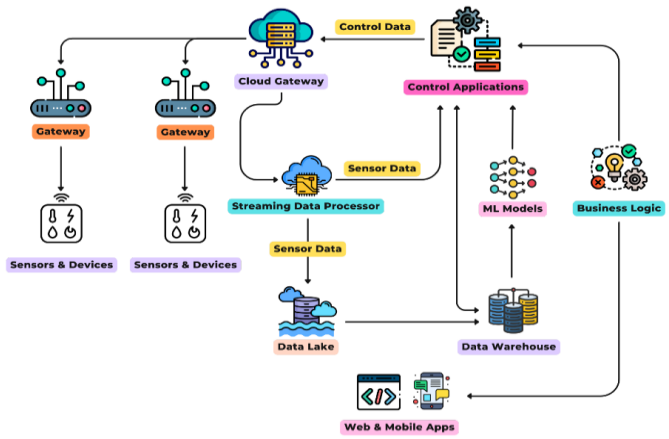

Figure 4: IoT System Design

(Source: https://www.mdpi.com)

Implementation and Deployment

Integrating with IoT Ecosystems

The compatibility issues, real time nature of security updates and lack of resources, makes it easier said than done to integrate scalable security configuration systems with IoT ecosystems. Speaking of the unification process, it is initiated by the assessment of the infrastructure in place, the establishment of risk and refinement of security policies. Security layers that extend from TLS (transport layer security) and DTLS (datagram transport layer security) are used to secure the exchanges of data between the devices and the central managing systems (Gupta *et al.*2017). This makes the configuration updates of every real time, by the use of deployment pipes, in order to enhance effectiveness of existing security measures. Further, life monitoring and logging provisions are incorporated into the system to give constant visibility on how the system is performing as well as flagging of abnormality.

Automated Configuration Tools

Automation solutions are vital when it comes to setting up scalability of security solutions for IoT technology. These tools employ machine learning techniques to predict the interaction of the devices in the network and make suggestions on the best configurations of the equipment security parameters and enforcing organizational security policies at the same time. It implies that the tools at work automates time consuming activities such as vulnerability scanning and patch management reducing overall operational overhead while also improving the efficacy of security configurations (Vögler *et al.*2016). The integration of IoT devices with centralized management platforms ensures that they all attach to the same security policies.

Results

Improved Threat Detection

Scalable security configuration systems greatly improve the prospects of detecting and minimizing security threats in IoT environments. Real time data processing and high level analysis lead to the possibility of detecting irregularities and possible breaches that in turn will allow for a fast reaction towards new threats. The implementation of distributed structures reduces the latency and improves the application of security measures in the devices and systems (Hernández-Ramos *et al.*2015).

The case studies used also show that the organizations that have implemented these systems cut down the frequency of the security incidents and realized enhanced systems stability.

Performance Metrics

Assessments of how the proposed system will perform indicate enhanced parameters which includes rate of correct identifications, time taken and the consumption of resources. Experimentation scales show that the performance characteristics of the interconnected system are stable, making the use of the indicated solution efficient at the network scale (Puliafito *et al.*2015). Further, the employed tools for integration mean less interference and are helpful for enhancing organized operational activities.

Discussion

Security configuration systems for IoT devices proposed to resolve identified key issues of securing different and constantly evolving ecosystems represent the area of focus. Some of the benefits include the ability to easily detect any threats, real time flexibility and easy policy implementation all combine to improve the security of IoT networks. Nevertheless, the deployment of these systems raises several issues, which are interoperability of the various devices involved, compatibility with systems already in place and requirements for computation resources (Abera *et al.*2016). These elements call for better scalability strategies and organizations need special, effective solutions for adapting to larger and more complex loads. Data quality is another important factor here, because the presence of low quality data puts in question the results of the threat detection and policy enforcement in an organization. From an ethical point of view, there are strict issues depending on data protection and regulation point of view, this should be more transparent and should follow legal compliance. Industry actors such as the developers, leaders in the industry and policymakers need to cooperate to come up with efficient and effective solutions for the problem. With such threats in mind and through further research and development of the technologies discussed here, the scalable systems would create a safe and flexible IoT platform for dealing with future emergent threats.

Figure 5: IoT Threats and Attacks

(Source: https://www.mdpi.com)

Future Directions

The studies on extending the IoT security scaling architecture and design should consider the application of blockchain and AI in improving the security parameters. Blockchain will allow device configurations to have a record that cannot be tampered with, enhancing accountability. Introducing AI technologies including deep learning, will enhance the ability to detect abnormal activities and also can support the process of decision making, to make further enhancement to security (Dalipi *et al.*2016). Furthermore, the development of edge computing and 5G opens a window of a chance in improving the scalability and real time reaction of IoT security systems. Industry Partnership is critical in effort to work towards creating solutions to modern security threats in IoT systems.

Conclusion

Security management solutions for creating scalable configurations are necessary for protecting IoT environments from new and growing threats, as well

as for maintaining the dependability of devices. Hence, these systems offer strong and flexible safeguards to corporate the challenges of developing IoT projects on an enormous scale. Specifically, the characteristics of the proposed framework reveal increases in threat identification effectiveness, activity productivity and conformance to guidelines. In addition to implementation and resource problems, the findings suggest that scalable systems could revolutionize IoT security. Additional investments in research, in combination with technology adoption will define further maturation of the safe IoT environment. As this report suggests, Industries must work together to address challenges affecting scalable and resilient security configurations in order to achieve a safer global society.

REFERENCES

[1]. Shaik, M., Venkataramanan, S., Sadhu, A.K.R. and Gudala, L., 2017. Envisioning Secure and Scalable Network Access Control: A Framework for Mitigating Device Heterogeneity and Network Complexity in Large-Scale Internet-of-Things (IoT) Deployments. Distributed Learning and Broad Applications in Scientific Research, 3, pp.1-24.

[2]. Noorman, J., Bulck, J.V., Mühlberg, J.T., Piessens, F., Maene, P., Preneel, B., Verbauwhede, I., Götzfried, J., Müller, T. and Freiling, F., 2017. Sancus 2.0: A low-cost security architecture for iot devices. ACM Transactions on Privacy and Security (TOPS), 20(3), pp.1-33.

[3]. Cirani, S., Davoli, L., Ferrari, G., Léone, R., Medagliani, P., Picone, M. and Veltri, L., 2014. A scalable and self-configuring architecture for service discovery in the internet of things. IEEE internet of things journal, 1(5), pp.508-521.

[4]. Li, F., Vögler, M., Claeßens, M. and Dustdar, S., 2013, June. Efficient and scalable IoT service delivery on cloud. In 2013 IEEE sixth international conference on cloud computing (pp. 740-747). IEEE.

[5]. Sarkar, C., SN, A.U.N., Prasad, R.V., Rahim, A., Neisse, R. and Baldini, G., 2014. DIAT: A scalable distributed architecture for IoT. IEEE Internet of Things journal, 2(3), pp.230-239.

[6]. Jiang, H., Shen, F., Chen, S., Li, K.C. and Jeong, Y.S., 2015. A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 49, pp.133-141.

[7]. Gupta, A., Christie, R. and Manjula, R., 2017. Scalability in internet of things: features, techniques and research challenges. Int. J. Comput. Intell. Res, 13(7), pp.1617-1627.

[8]. Vögler, M., Schleicher, J.M., Inzinger, C. and Dustdar, S., 2016. A scalable framework for provisioning large-scale IoT deployments. ACM Transactions on Internet Technology (TOIT), 16(2), pp.1-20.

[9]. Hernández-Ramos, J.L., Moreno, M.V., Bernabé, J.B., Carrillo, D.G. and Skarmeta, A.F., 2015. SAFIR: Secure access framework for IoT-enabled services on smart buildings. Journal of Computer and System Sciences, 81(8), pp.1452-1463.

[10]. Puliafito, A., Celesti, A., Villari, M. and Fazio, M., 2015. Towards the integration between IoT and cloud computing: An approach for the secure self-configuration of embedded devices. International Journal of Distributed Sensor Networks, 11(12), p.286860.

[11]. Abera, T., Asokan, N., Davi, L., Koushanfar, F., Paverd, A., Sadeghi, A.R. and Tsudik, G., 2016, June. Things, trouble, trust: on building trust in IoT systems. In Proceedings of the 53rd Annual Design Automation Conference (pp. 1-6).

[12]. Dalipi, E., Van den Abeele, F., Ishaq, I., Moerman, I. and Hoebeke, J., 2016, December. EC-IoT: An easy configuration framework for constrained IoT devices. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 159-164). IEEE.