International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21742

An Edge Driven Security Framework For Intelligent Internet Of Things

Nikhil H R[1], Ruthwik B G[1], Sampath L S[1], Sourabh R[1] , Narender M[2]
[1]Student, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India
[2]Assistant Professor, Department of Computer Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India

Article Info
Volume 7, Issue 4
Page Number: 27-31

Publication Issue :
July-August-2021

Article History
Accepted : 25 June 2021
Published : 02 July 2021

ABSTRACT

The use of IoT technologies has increased from 13 percent in 2014 to about 25 percent today. And around the world number of IoT-connected devices is expected to increase to 43 billion by 2023, a threefold increase from 2018. IoT will continue to grow in device numbers and use cases, but organizations must reckon with the security and interoperability challenges that have plagued the market since the beginning. Building robust IOT applications by incorporating security features has become a necessity. Thus, in this article, an edge-driven security framework architecture is described for intelligent IoT systems. A security framework contains all standard security features required by an application such as authentication, authorization, secure connection etc. We introduce the architecture of edge-driven intelligent IoT, and present typical edge-driven intelligent IoT applications. Second, we point out the security threats in edge-driven intelligent IoT in terms of attack behaviour of adversaries. Third, we develop a case study of edge-driven intelligent IoT from the security perspective. Our focus is to develop a middleware or framework between the Users and IoT Environment to ensure users are connected to IoT environment upon authentication for a contract session and create secure communication via cloud between the users and IoT environment

Keywords : Internet of things, Security Framework, API, asp.net , webservices

I. INTRODUCTION

The Internet of Things interconnects computer devices integrated in everyday objects through the Internet, allowing them to send and receive data. There are two-fold advantages, we can empower our computers to gather information about surroundings without depending on humans and by processing the information collected we can reduce extravagance, loss, and cost. The Internet of Things allows for interaction between the physical world and the digital World. The digital world interacts with the physical world via sensors and actuators. These sensors collect information that must be stored and processed. Data processing can take place at the edge of the network or at a remote server or cloud. The storage and processing capabilities of an IoT object are restricted by the resources available, which are

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

constrained due to size limitation, energy, power, and computational capability. So these systems rely on IoT middleware to provide needed capabilities.

APIs allow exposing the connected device to users in a secure manner. REST full APIs are widely being used in the modern web. Data transfer is usually done using JSON or XML over HTTP. It is a good model for the heterogeneous systems. REST API makes the device information easily available. They can standardize on a way to create, read, update, and delete this data. All these operations will be input to the REST query calls. REST APIs allow to delegate and manage authorization. The API can authenticate on the server and the server can authenticate to the API to prevent the man-in-the-middle attacks.

One way to handle such heterogeneous applications is that we can have a middleware platform that will become the Bridge between things and applications in the cloud. Middleware packages and abstracts hardware, and provides application programming interfaces (APIs) for communication, data processing, computing, privacy and Security.

II. LITERATURE SURVEY

Zhou Su Shanghai University, Shanghai, China Ruidong Li National Institute of Information and Communications Technology, Koganei, Japan[1]

Describes with the increasing use of the Internet of things (IoT) in diverse domains, security concerns and IoT threats are constantly rising. The computational and memory limitations of IoT devices have resulted in emerging vulnerabilities in most IoT-run environments. Due to the low processing ability, IoT devices are often not capable of running complex defensive mechanisms[2]. Lack of architecture for a safer IoT environment is referred to as the most important barrier in developing a secure IoT system. In this paper, we propose a secure architecture for IoT edge layer infrastructure, called AI4SAFE-IoT. This architecture is built upon AI-powered security modules at the edge layer for protecting IoT infrastructure. Cyber threat attribution, intelligent web application firewall, cyber threat hunting, and cyber threat intelligence are the main modules proposed in our architecture. The proposed modules detect, attribute, and further identify the stage of an attack life cycle based on the Cyber Kill Chain model. In the proposed architecture, we define each security module and show its functionality against different threats in real-world applications. Moreover, due to the integration of AI security modules in a different layer of AI4SAFE-IoT, each threat in the edge layer will be handled by its corresponding security module delivered by a service. We compared the proposed architecture with the existing models and discussed our architecture independence of the underlying IoT layer and its comparatively low overhead according to delivering security as service for the edge layer of IoT architecture[4] instead of embed implementation. Overall, we evaluated our proposed architecture based on the IoT service management score. The proposed architecture obtained 84.7 out of 100 which is the highest score among peer IoT edge layer security architectures.

J. Sathish Kumar et al: author presented Internet of Things with architecture and design goals. They surveyed security and privacy concerns at different layers in IoTs. In addition, they identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. It was also discussed the applications of IoTs in real life. In future, research on the IoTs will remain a hot issue. Lot of knotty problems is waiting for researchers to deal with [3].

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

It is very difficult for any application developer to design an application right from the scratch. It takes lot of time and effort. And this will increase the complexity for the developer. In existing system in order to realize inter connection among devices and services in the IoT, interoperability of APIs is considered an Important challenge Generally speaking, IoT devices from different vendors provide different APIs, which are non customizable and device-specific. Because of this, application developers need to understand the API specifications of each device and write specific codes to integrate these devices. For example, if you replace an air conditioner with another from a different manufacturer, a smart house application needs to be upgraded as well to support the new one, even though both provide the same functionality. Such updates in household devices can often happen, which makes interoperability in IoT crucial. So far, much work has been done to address this problem, and it can be classified into two categories: semantic and syntactic approaches The first tries to describe semantics of device APIs as device profiles using Resource Description Framework derived from the semantic web. By utilizing the device profiles, programs can understand the meaning of API, how to use it, which can be used to convert an API to another. However, it is considered impractical to process description logics for API conversion, due to its high computational cost and its limited readability. On the other hand, the latter approach tries to describe API specifications syntactically, which enables device profiles to be handled efficiently. However, none of the existing work based on syntactic approach is flexible enough to make device APIs interoperable.

B. PROPOSED SYSTEM

In order to over the problems of existing system we propose a novel framework for the Internet of Things (IoT) devices, which aims to realize interoperability among devices without modification to the devices. Our framework works as a proxy that accepts standard API requests, which are translated into device-specific requests using the conversion rules defined as device-specific profiles. Application programmers are not required to be aware of the difference of the APIs of devices thanks to the standard API provided by the framework.

We evaluated our framework and found that our framework can standardize two different device APIs in practical scenarios with a negligible impact on response time.

Here in this method there will be 2 actors, one is the frame work developer and another one is the application developer. Where the frame work developer will be reducing the complexity of developing the application by the application developer. That means most of the frame works are already been designed by the frame work developer the application developer needs to just make use the frame work which is already been developed by the application developer. This process helps to reduce the time and complexity for the application developer, he no need to do the things right from the scratch . frame will already be there which are ready to use.

IV. SYSTEM DESIGN

After analyzing the system, we need to design the system according to the need and requirement of the user. Various design techniques are adapted to exhibit the flow of data.System design is the process of defining the architecture, components, modules,

interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. Architecture focuses on looking at a system as a combination of many different components, and how they interact with each other to produce the desired result. The focus is on identifying components or subsystems and how they connect as show in Fig1.

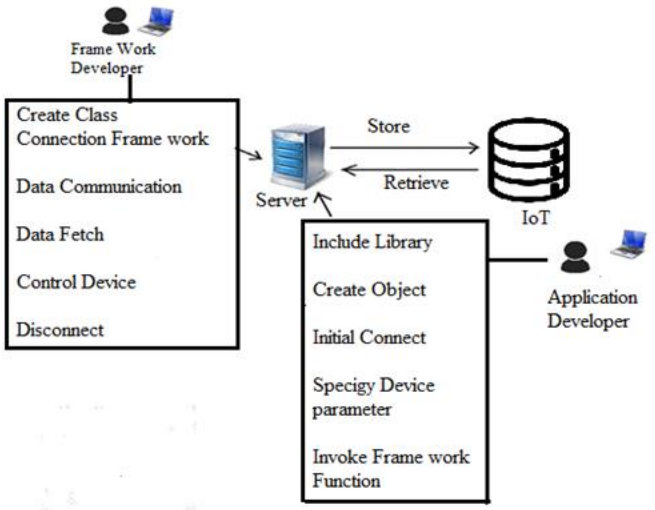

Fig. 1 – System Architecture

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes as well as the data flows intersecting with the related activities show in Fig.2 and Fig.3

Fig. 2 – Framework Developer Activity Diagram

Fig. 3 – Application Developer Activity Diagram

V. SYSTEM IMPLEMENTATION

A crucial phase in the system lifecycle is the successful implementation of the new system design. Implementation simply means converting a new system design into operation. Implementation is a stage in which the design is converted into working system. Implementation is the process of bringing the developed system into operational use and turning it to the user. This stage is considered to be the most crucial stage in the development of a successful system since a new system is developed and the users are given the confidence of its effectiveness.

Implementation Phases are as follows:

- First phase includes table design for Database module.
- Second phase includes coding for GUI modules
- Third phase includes the integration of modules
- Fourth phase includes connection establishment between the front-end and back-end
- Fifth phase includes error handling and message generator.

VI. CONCLUSION

In this article, we have investigated an edge-driven security framework in intelligent IoT systems. First, we have introduced an edge-driven intellgent IoT architecture that incorporates the data generating layer, the edge computing layer, the cloud computing layer, and the application layer. Second, we have presented several intelligent IoT applications based on edge computing. The security threats in edge-driven intelligent IoT systems have been discussed.

The future technology itself seems very bright, the reason being that it brings to the table what no other technology brings. What web service provides is a platform where multiple organizations can collaborate, exchange data, performs transactions in a secure, trusted and immutable fashion.. Webservice brings all this together to form a holistic system, providing a platform which multiple organizations can use to share data, automate tasks across organizations using smart contracts and much more. All these makes this application a very powerful technology, leading to a potentially extremely bright future. Now where can this be used? Any domain which has multi parties transacting with each and where there is lack of trust between the parties involved, this technology can help. Some of the famous domains are F&A, Supply chain management, governance, KYC, Mortgage processing and the list is endless.

VII. REFERENCES

[1]. W. Li et al., “Defending Malicious Check-In Using Big Data Analysis of Indoor Positioning System: An Access Point Selection Approach,” IEEE Trans. Network Science and Engineering. DOI: 10.1109/TNSE.2020.3014384.

[2]. D. He, S. Chan, and M. Guizani, “Security in the Internet of Things Supported by Mobile Edge Computing,” IEEE Commun. Mag., vol. 56, no. 8, Aug. 2018, pp. 56–61.

[3]. J. M. Jimenez et al., “MHCP: Multimedia Hybrid Cloud Computing Protocol and Architecture for Mobile Devices,” IEEE Network, vol. 33, no. 1, Jan./Feb. 2019, pp. 106–12.

[4]. W. Li et al., “Abnormal Crowd Traffic Detection with Crowdsourcing-Based RSS Fingerprint Position in Heterogeneous Communications Networks,” IEEE Trans. Network Science and Engineering. DOI: 10.1109/TNSE.2020.3014380.

[5]. D. Puthal et al., “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing,” IEEE Commun. Mag., vol. 56, no. 5, May 2018, pp. 60–65.

Cite this article as :

Nikhil H R, Ruthwik B G, Sampath L S, Sourabh R, Narender M, "An Edge Driven Security Framework For Intelligent Internet Of Things", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 4, pp. 27-31, July-August 2021. Available at doi : https://doi.org/10.32628/CSEIT21742

Journal URL : https://ijsrcseit.com/CSEIT21742