International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206283

Lightweight Authentication Protocol in Internet-of-Things

Anamika A. Mishra[1], Krushnalee Surve[1], Devika C. Babu[1], Upendra Verma[2]
[1]Department of Computer Science, SVKM's Narsee Monjee Institute of Management Studies, Mukesh Patel School of Technology Management and Engineering, Shirpur, Maharashtra, India
[2]Assistant Professor, SVKM's Narsee Monjee Institute of Management Studies, Mukesh Patel School of Technology Management and Engineering, Shirpur, Maharashtra, India

ABSTRACT

Internet of Things is the extension of Internet connectivity into physical devices, called IoT devices which are connected to Cloud Servers, which help them perform many functions, including, but not limited to security protocols. However, the distance between the Cloud Server and the end device could hamper the connectivity and also risk the security. Authentication is one of the major issues that needs to be taken care of in this scenario. This paper aims to look into this issue as well as to provide a viable solution.

Keywords : Cloud Computing, Internet of Things, Authentication, RSA, AES - 128 bit

I. INTRODUCTION

Internet of Things involves the extension of the Internet into everyday physical devices. These devices are called Internet-of-Things devices or just, IoT devices. These devices are connected to a Cloud Server, on the basis of which the end devices are able to perform an extensive amount of computational operations . [1] The various activities include storing and managing data, administering the network connection, even tending the security measures for the same. However, the distance between the Cloud Server and the end device is massive. This compromises the connectivity of the network in terms of security and reachability. Authentication is the prime concern that needs to be addressed in this scenario.

Authentication protocols are generally carried out by the straightword connections between IoT devices and the Cloud Server. Moreover, due to changing technologies it is not possible to adopt the traditional security measures as the new end devices are highly resource constrained due to portability. Fog Computing is one such architecture that helps overcome these problems. [3]

Hence, here we establish a fog node, which helps with the authentication and authorisation of the IoT Device with the cloud server as well as enhances the security between these two entities. The fog node helps create a low-latency network which helps in the fast computational processing of delay-sensitive data. [6]
Investopedia states that Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.

The CISCO's definition for fog node is that it extends the cloud to be closer to the things that produce and act on IoT data These devices, called fog nodes, can be deployed anywhere with a network connection.

According to ZDNet definition, the Internet of Things, or IoT, refers to the billions of physical devices around

the world that are now connected to the internet, all collecting and sharing data.

The two main factors of utter importance , is the fast working of the end devices and the security of the data that is stored and processed by these devices.

Our paper offers a solution for both of the aforementioned issues. The Lightweight Authentication Protocol aims to reduce the network-latency and bandwidth issues of delay-sensitive data using a fog node. It is designed for the transfer of authenticated data between two entities. It allows the receiving entity to authenticate the connecting entity as well as to authenticate itself to the connecting entity by declaring the type of information needed for authentication as well as syntax. [5] This helps strengthen the security, as the security of the connection between the end device and the Cloud Server is of utmost importance. If the security is compromised, the repercussions could be devastating. For example, improper security of an end device to cloud connection can lead to fraud, waste and abuse in healthcare that ranges from deliberate manipulation of data to increase bill amounts or false insurance claims to fictitious medical records. This has a humongous impact globally. According to the Global Healthcare Anti-Fraud Network, approximately $260 billion, which is 6% of global healthcare spending is lost to fraud each year. [7] Thus, additional security can also be provided through alphanumeric or biometric passwords. The security of the system is evaluated on the basis of Confidentiality, Integrity and Availability.

II. SCOPE

The Lightweight Authentication Protocol aims to reduce the network-latency and bandwidth issues of delay-sensitive data using a fog node. The above mentioned problems occur due to heavy congestion on the network and the resource rich characteristic of the cloud. It is designed for the transfer of authentication data between two entities. [1] It allows the receiving entity to authenticate the connecting entity as well as to authenticate itself to the connecting entity by declaring the type of information needed for authentication. The purpose of implementing lightweight protocol is:

1. To find out which algorithm(s) are best for establishing the connection between IoT devices and the fog node.
2. To access the response-sensitive data without any latency.
3. To solve the issues of Things-To-Cloud connectivity.
4. To save network bandwidth by processing selected data at the fog node.
5. This project is aimed at applications such as Smart Traffic Light System or Critical Healthcare Systems.

Latency and bandwidth constraints are the main issues faced by the connection between an IoT device and its respective Cloud Server. To overcome these issues, a fog node is utilized and implemented between the two entities.. The purpose of the fog node is to store important data that is the delay sensitive data and provide the end device with this data when required, as well as, to authenticate the end device and uphold the security of the connections between the end device, the fog node and the cloud server. [3]

Hence, the Lightweight Authentication Protocol is implemented. The purpose of this implementation is to use authentication protocols to establish a connection between the IoT device, fog node and cloud node, using Advanced Encryption Standard and Rivest-Shamir-Adleman algorithms which are lightweight in nature. [4]

III. PROBLEM STATEMENT AND PROPOSED SOLUTION

The problem statement can be described as the following:

1. Traditional Authentication mechanism cannot be used for a resource-constrained environment.
2. The network connections between an IoT Device and a Cloud Server require a certain level of openness as well as very limited human intervention.
3. The major issues in the connectivity of an IoT Device to a Cloud Server are:
   a. Latency
   b. Bandwidth Constraints
   c. Network Traffic

The objective of this project is to develop a Lightweight Authentication Protocol that improves the security of the connection between an IoT Device and a Cloud Server and to overcome the problems of latency and bandwidth of the existing cloud model. The Fog Computing architecture helps create a low latency network by establishing a device, called a Fog Node, between the IoT Device and the Cloud Server. [2]

This proposed authentication protocol, since lightweight, makes use of symmetric as well as asymmetric cryptography. This project makes use of the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) cryptographic algorithms for this purpose. [4]

The issues of Things-to-Cloud connectivity are resolved by establishing a connection between the end-devices and a fog node. To validate the connection between the end-device and the fog node, a lightweight authentication protocol is run, which operates on the basis of symmetric cryptography, which has been implemented using 128-bit Advanced Encryption Standard (AES), this helps decrease the latency and omits unnecessary congestion by allowing small computational operations to be done there itself. [3] The fog node is connected to the Cloud Server through asymmetric cryptography. The algorithm used for this connection is the Rivet-Shamir-Adleman (RSA) algorithm. This algorithm is used to improve the security of the connection and hence avoid security breaches.

IV. DESIGN

The proposed architecture is as follows:

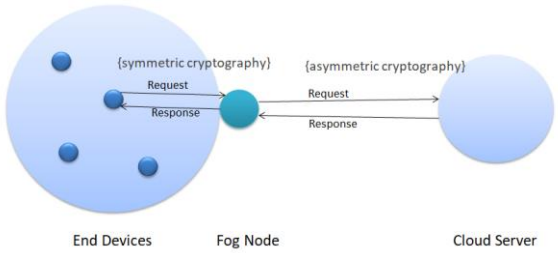

Fig1: Proposed Architecture

The architecture is realised with the help of several software development diagrams. The diagrams are represented as follows:

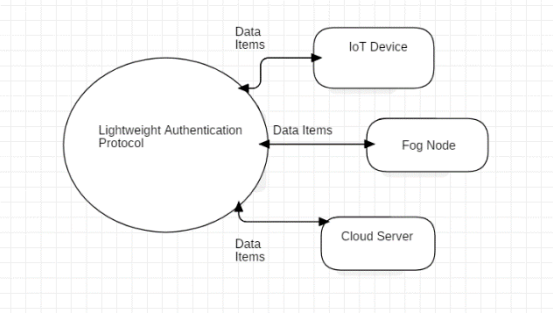

Fig 2: Level-0, Data Flow Diagram

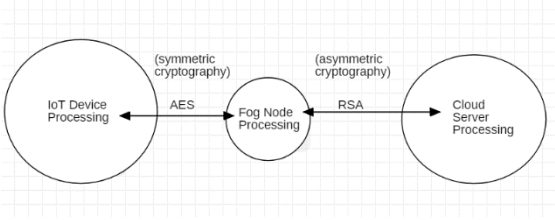

Fig 3: Level-1, Data Flow Diagram

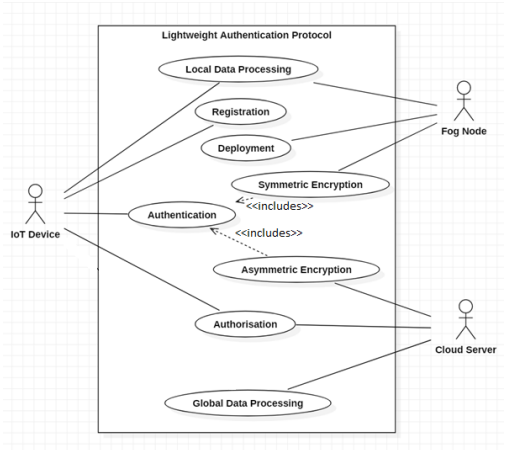

Fig 4: Use Case Diagram

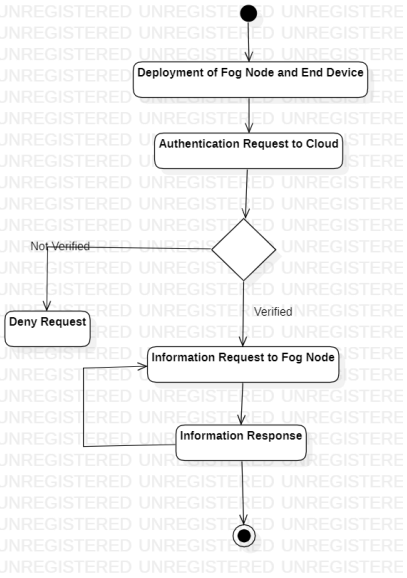

Fig 5: Activity Diagram

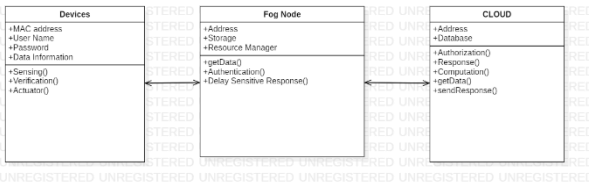

Fig 6: Class Diagram

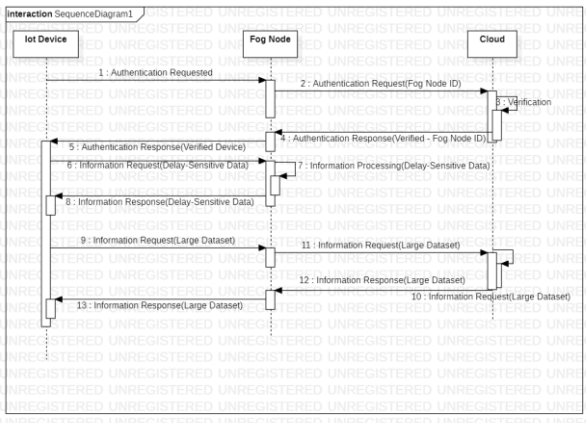

Fig 7: Sequence Diagram

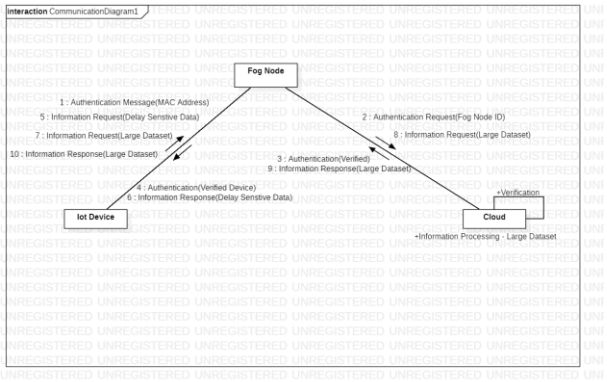

Fig 8: Collaboration Diagram

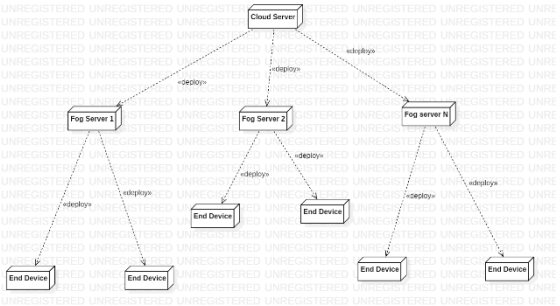

Fig 7: Deployment Diagram

V. CONCLUSION

The paper reviews the essential security concerns of a Device-to-Cloud connection and offers a solution to overcome these concerns. The low latency network established in the supporting project helps in fast processing of delay-sensitive data. Hence, this project is intended for delay sensitive data applications such as Smart Traffic Lights, Critical Medical Analytics, etc. This project will be useful for receiving quick responses with the highest standards of authentication.

VI. REFERENCES

[1]. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2017). A comprehensive survey on fog computing: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 20(1), 416-464

[2]. G. Shanmugasundaram, V. Aswini, G. Suganya, "A Comprehensive Review on Cloud Computing Security", International Conference on

Innovations in Information, Embedded, and Communication Systems (ICIIECS), 2017.
[3]. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal, 3(6), 854-864.
[4]. Patra, L., & Rao, U. P. (2016, March). Internet of Things—Architecture, applications, security and other major challenges. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 1201-1206
[5]. Farooq, H. (2017). A review on cloud computing security using authentication techniques. International Journal of Advanced Research in Computer Science, 8(2).
[6]. Prakash, A., & Kumar, U. (2018). Authentication Protocols and Techniques: A Survey.
[7]. National Healthcare Anti-Fraud Association, United States of America

Cite this article as :

Anamika A. Mishra, Krushnalee Surve, Devika C. Babu, Upendra Verma, "Lightweight Authentication Protocol in Internet-of-Things", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 271-275, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT206283
Journal URL : http://ijsrcseit.com/CSEIT206283