# A TOKEN-BASED AUTHENTICATION SYSTEM THAT IDENTIFIES USERS AND DEVICE IN AN IOT APPLICATION/ECOSYSTEM

[1]B. Bamleshwar Rao, [2]Dr. Akhilesh A. Waoo

[1]Research Scholar, [2]Associate Professor,
[1]Department of Computer Science,
[1]AKSU, Satna(M.P.), India.

***Abstract:*** This study has been undertaken to understand the importance and need of security as a critical consideration while framing any IoT architecture or an ecosystem for an application. With this consideration, the abstract comes with a solution to leverage the capabilities of using token-based authentication to identify the users and devices which the Token-Based authentication provides secured and reliable data with the help of sensors and the sensors pass authentic information of the users to the device in the form of secured data for the particular purpose which could be used to draw and reach up to the relevant conclusions.

***IndexTerms*** **-** Authentication, Cryptography, Ecosystem, IoT, MQTT, PAN, Protocol, Security, Token.

## I.INTRODUCTION

The Internet of Things (IoT) is the connection of devices to the Internet and other connected devices. All of these devices share data about the way they are used and about the environment around them **[1]**. Communication being the backbone of this ecosystem is brought to reality using networking technologies. These Networking technologies enable the IoT devices to be connected with various other IoT devices, applications, and various other cloud services running on the cloud. In this heterogeneous ecosystem, communication is brought by the help of the internet which relies on various standardized protocols that define various rules and formats for these devices as a must follow to establish and manage the transmission of data across those networks. Modern networks are selected and built with a bundle of technologies arranged in a manner that they stand optimal to the use case of the IoT application. There are various consideration and challenges one has to be mindful of while establishing an IoT application, these majorly include:

### 1.1 Range

The network should be capable of retrieving data from the various IoT devices and transmit it to its intended destination this could be a data center or simple a hosted service from where this data is processed. Considerations have to be made to employ a given network that suits the use case and scenario of the application. For example, a Bluetooth based communication between devices would be best for an application where all devices communicate are placed within a room or a very few meters apart this is a case of Personal Area Network (PAN) but this won't be working If the communicating devices of the application are situated thousands of kilometers apart. In this case where transmitting data over a required range becomes a challenge, leveraging edge computing, where data is analyzed directly from the devices and not from a data center would be a workaround.

### 1.2 Bandwidth

At times, the Responsiveness of an IoT application is limited only due to the capabilities of the system which may be

- Physical such as carrier frequencies, medium's spectrum sharing between various devices and their services for transmitting data or
- Logical such as programming techniques, overheads, and security checks are employed to make the system software devices.

It arrives at the fact bandwidth is dependent on various factors such as the volume of data being gathered and transferred, the number of devices deployed in a particular application, in what manner data is being transmitted i.e. Is it transmitted as a continuous stream of data or small packets of data in intermittent bursts?

### 1.3 Power Consumption

A factor that is challenging and has to be considered for the devices deployed at remote geographical locations or which create their energy to be up and working.

### 1.4 Security and Interoperability

Devices and Services work with each other to bring the system's intended output and use. This is called Interoperability which is achieved by standardizing protocols to be used at different layers of processing, transmission, and reception as data flows from one end to another. With a wide range of devices, IoT adds more to this already versatile forest of incompatibility and security issues. At times these are either hard to adopt with innovation and change. Having these handlers on physical (on device hardware)

or logical (on-device system software/program) adds to the processing overhead thus, affecting the overall efficiency of the IoT application.

Security is a priority if the application or IoT ecosystem as a whole is to be operated on a wide range of devices and has a critical effect on the diverse analysis of its produced data. The following factors shape a secure and safe IoT network **[3,4,5]**:

- **Authentication**
  Adopting secure protocols that authenticate the attached devices, users, gateways, services, and applications. Generally, it is considered to adopt the X.509 standard for device authentication.

- **Encryption**
  The involvement of this technique ensures privacy and data integrity for communication as data flows through various platforms.

- **Port Protection**
  Ensuring that only the ports and the services hosted on them that participate in communication are made available as open to the external connections. Rest all services are in abstraction and are protected by firewall rules.

## II.NEED AND SIGNIFICANCE OF RESEARCH

Every time a device or service communicates i.e. transmits or receives data there is a potential risk of the data being manipulated by various participating or external streams which may be physical or logical and maybe for a mischievous intention **[2]**. This tampers the information that was intended to be sent and if critical analysis is made over such data, this could have adverse effects on how maybe a government makes decisions for the people of its country.

Authentication plays an important role here as to who should be having access to data where the analysis of this data can be made to make some critical decisions. Consider the case of weather forecast using IoT, where network-enabled devices equipped with sensors are deployed at various geographical locations to collect and publish some weather parameters such as wind speed, air quality index, humidity, light, rain, etc. to their central server from where the analysis to forecast the next day's weather would be made. Here data would have been collected and transferred from one device to others in every intermediate stage and only the analysis i.e. weather forecast could become the interest. It is due to this the need for devices and services authenticating their identity and verifying that to whom they are streaming the information.

## III.OBJECTIVE

- The existing authentication systems mainly involve human input to provide either password, One-time-password (OTP), push notification approval, QR code scan on an already authenticated device to establish ones' identity for verification and this cannot be implemented one a device to device authentication as it is supposed to be automated and essentially driven with a security measures taken into account. Hence, the objective is to design a token-based authentication system that identifies users and devices in an IoT application/ecosystem.
- The analysis focuses on distinguishing and upgrading existing security frameworks, initiatives that are designed to be applied to IoT.
- Device security is mainly about ensuring that a trusted set of devices participate as a part of the system. Also, on the other hand, these devices trust the broker or application sending commands to them.
- The same goes for the users in the system as only the legitimate users participate to operate in the system.
- Having an access token-based mechanism to attain the trust with various stages of data flow can help here as an automated device to device authentication will be possible without human intervention.
- A popular messaging protocol and widely used and supported by key players in the market is Message Queuing Telemetry Transport (MQTT). It works on top of TCP/IP protocol and is designed for connections with remote locations where a small code footprint is required or network bandwidth is limited **[5]**.
- MQTT is a lightweight publish and subscribe messaging protocol for an end device/application termed here as a client.

## IV.TOKEN-BASED DEVICE & USER AUTHENTICATION

The analysis is to enhance the robustness of authentication, various Security analyses conclude that such a scheme is a strong competitor among the existing one for device and user authentication in IoT systems(fig. 1). This includes performance analysis as well **[6]**.

A token is a string that the server generates for the client that can be passed over as a plain text over a selected protocol generally inside an HTTP request (over the internet).

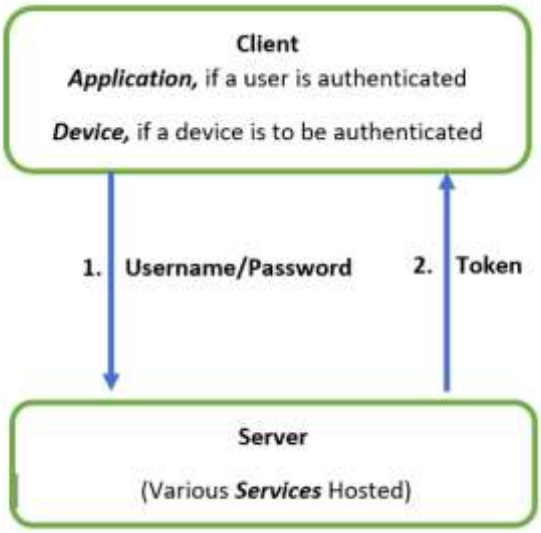


**Figure 1** User Authentication

The idea is that the client application/device exchanges authentication credentials for an authentication token(fig. 2). In subsequent requests or streaming, data just sends the token **[7]**.

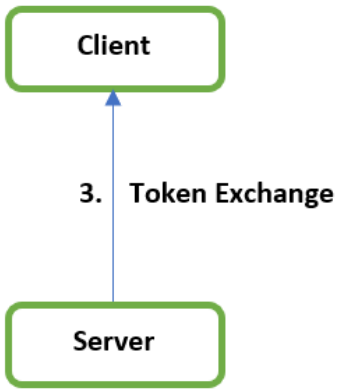


**Figure 2** Token Exchange

## V.IMPLEMENTATION OF TOKENS GENERATION

A general approach is to generate a random sequence of characters of a certain length that is stored at the username and password in the application server's database along with the expiration timestamp, As shown in Table 1. The token here is plaintext and can be easily verified with a regular programmatic string comparison method with a check on the expiration date.

Table 1: Details of User Authentication

| | |
|---|---|
| Username | User1 |
| Password | P@$$word |
| Token | QWERTY123 |
| Expiration | 12:00 PM |

A more elaborate implementation that requires no server-side storage is to use a cryptographically signed message as a token. Its advantage would be that for which user/device Id the token is generated is encoded in the token itself and protected against tampering with a strong cryptographic signature.

## VI.CONCLUSIONS

IoT is getting smarter, more distributed, and diverse from smart homes to smart cities. The IoT will grow in the context of security capabilities, but computer security outlook is to change under the pressure of IoT. This technology can be used to record events such as sensor data which can be made to be datasets for artificial intelligence routines.

Massive adoption brings new problems and requires that devices in the IoT ecosystem incorporate security as a key design element and not just an afterthought **[9]**.

## VII. REFERENCES


**[1]** IBM developer Articles: Connecting all the things in IoT, *January 31, 2020*

**[2]** IBM developer Articles: Minimizing application privacy risk, *May 25, 2018*

**[3]** IBM developer Articles: Securing IoT devices and Gateways, *February 28, 2018*

**[4]** IBM developer Articles: Securing IoT data over network, *February 28, 2018*

**[5]** IBM developer Articles: Securing IoT data over network, *February 28, 2018*

**[6]** Architectural design of token-based authentication of MQTT protocol in constrained IoT device: Adhitya Bhawiyuga, Mahendra Data, Andri Warda Publisher: IEEE. **INSPEC Accession Number:** 17543247

**[7]** Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review Volume 2019 |Article ID 9629381.

**[8]** Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model.Evidence from KSE-Pakistan.European Journal of Economics, Finance and Administrative Science, 3 (20).

**[9]** S. Hameed and H. A. Khan, "SDN based collaborative scheme for mitigation of DDoS attacks," Future Internet, vol. 10, no. 3, p. 23, 2018