ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 9; Issue 3; May-June; 2021; Page No. 01-06

QR CODE BASED MULTI FACTOR AUTHENTICATION PROTOCOL FOR IoT NETWORKS

B. Prema Sindhuri

Assistant Professor, Department of CSE, Presidency University, India

Conflicts of interest: Nil

Corresponding author: B. Prema Sindhuri

Abstract

In recent years, with rapid growth and development in Internet of Things (IoT) Technology using wireless communication networks. There are major applications like smart home, smart health care and smart transportation etc. Generally the IoT devices access the user private data, the security and privacy become a challenge. As we are having various authentication systems implemented for authorizing the user to get the access of device or to get the controls of device. Multi-factor authentication (MFA) provides great security to the device. QR code is a 2D matrix code provides high data store capacity than bar code. Now a days, QR code is applied in many applications like payment systems, security etc. The proposed architecture implements the security enabled IoT device, in order to get the access or controls it requires MFA which is encrypted QR code.

Keywords: Encrypted QR Code (EQR Code), IoT, Key Pair, Multifactor authentication.

1. Introduction

IoT Overview:

The things which are connected to the internet and which allows anyone to access anywhere at any anytime using any path/network and service is called Internet of Things(IoT). For Example, Cam scanners, QR code scanners, laser scanners, RFID tags, Infrared sensors and some other sensors are connected to the object for communication and data exchange services. And for track the application, monitor and to handle the devices the physical infrastructure IoT is needed.

Security issues for IoT:

As earlier discussed all IoT devices and the people are connected to the internet to communicate and to provide the services at any time. But most of the devices are not having security services and mechanisms e.g., Authentication, Confidentiality, Integrity etc[1]. The IoT devices contains different network with different platform having different credentials. The privacy of the user identity and his information is very important because the personal information is shared among various network of devices. Hence a secure mechanism is required to protect the information.

Security Services in IoT:

The IoT has many security requirements as follows [2]:

i. Confidentiality: It refers to protect the information from being accessed by unauthorized persons or parties. In IoT environment, authorization is provided for not only for the users, also for the objects. So it needs to address the both the object authentication and access control mechanism.

ii. Integrity: It refers to the honesty, reliability and trustworthiness of data. In IoT Environment, as the devices and users are connected to the

network. An opponent may alter the data when the sensitive data is transmitted from the device to the user. So, it needs a trusted application to maintain the integrity of data.

iii. Availability: It refers to that information is provided by authorized users. In IoT environment, the large amount of data will be available everywhere. Everybody can access the generated data by any device. So, it needs a proper algorithm to ensure the availability of data and services.

iv. Non-Repudiation: It refers to the validity of information or assurance that someone cannot deny the validity. In IoT environment, a node or object cannot deny its message or data that has been sent to the user or another node. So, it needs a data ownership to access the device.

v. Authorization: It refers to the privileges for the user or object to access the data or control related to the system resources, services and application features. In IoT environment, with proper identity anybody can get the control of device and also can access the information. So, it needs a high authentication and identity verification to tighten the application.

In recent case [3], there is lack of security addressed in the Nissan LEAF. There anyone can access the data from the registered car using internet like the how many trips and how much distance travelled in each trip on that day, and the timings etc. In addition to that he can get the control of the AC in the car. This is because of lack of proper authentication. An opponent just need the vehicle identification number (VIN) which will be present in the front of car. So, in this proper mainly the security provided to the application in terms of authentication [4].

Authentication: It is the process of checking the identity of the user or object participated in the communication. In IoT environment, it is necessary to provide an authentication for the devices and also to the users. And it also works along with the confidentiality, integrity and authorization. There are several types of authentication [5].

Types of Authentication:

i) Single factor authentication: It is also called as primary authentication which is very simple and most common form of the authentication. This type of authentication contains the methods like passwords, PIN etc. This method is easy for the opponent to steal the passwords and can get the access control for the application.

ii) Two factor authentication (2FA): Adding another security level to the single factor authentication. Common methods of 2FA are one time passwords (OTP's), or security PIN numbers. Mostly 80% of data breaches can be prevented by this mechanism.

iii)Multifactor authentication (MFA): It is the important authentication method that provides 2 more level security factors to permit the user grant of a system. General methods of MFA are fingerprint, faceID, local information, security token etc.

In this paper, the proposed system involves multifactor authentication using Quick Response (QR code).

Quick Response (QR) Code:

A QR code is a one type of bar code and it is a two dimensional matrix code which stores the information by considering two points [6]. It provides the high storage capacity which is represented in small size [7]. It is used for fast scanning to represent many types of data. It can also use in many applications like information security, payment, identification, marketing and advertising etc. It started to appear in marketing techniques in 2011-2012. Next it's started to appear in smart phones. It is represented as Fig 1.

Figure 1: QR Code

/

The QR code also having various versions starts from version1 to version 40[8]. Each version contains different module configuration refers to the number of modules. Version1 contains 21 x 21 modules whereas version 40 contains 144 x 144 modules. QR codes are categorized into five different categories [6].

i) QR code Model 1 & 2

ii) Micro Code

iii) LogoQ (Logo QR Code)

iv) iQR(i QR Code)

v) EQR(Encrypted QR Code)

In this paper, EQR will be used as a multifactor authentication. EQR, basically an encrypted QR code contains an encrypted data. The data information is encrypted by using cryptography techniques and applied to the generated QR Code.

2. Literature Survey

There are various existing system on IoT security and access control issues. Tobias Marktscheffel and Wolfram Gottschlich [3] summarizes that QR code based mutual authentication protocol between the device and the user. There is a protocol which provides a mutual authentication using QR codes. That protocol can be implemented in two ways either active authentication or passive authentication represented as below Fig 2 and 3[3]. In both versions it required a new device to scan the QR Code. The new device has to be connected with the master along with the registered device. When registered device or new device is requested for the QR code the master will generate the code by attaching the certificate using SHA256 as cryptographic algorithm to provide from the attacker. The importance of that protocol is mainly to protect the information from the network based attacker. That protocol supports two types of operation modes to handle the hardware configuration.

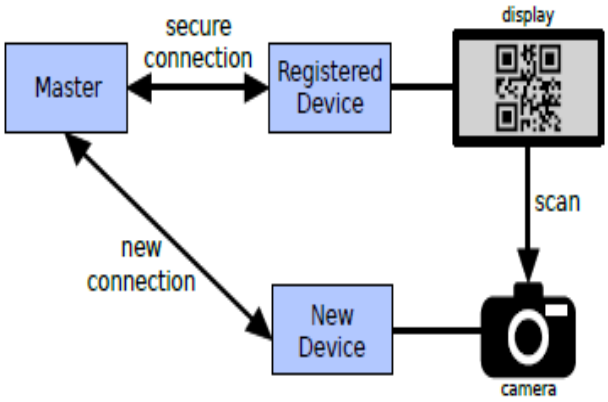

Figure 2: Active Scenario

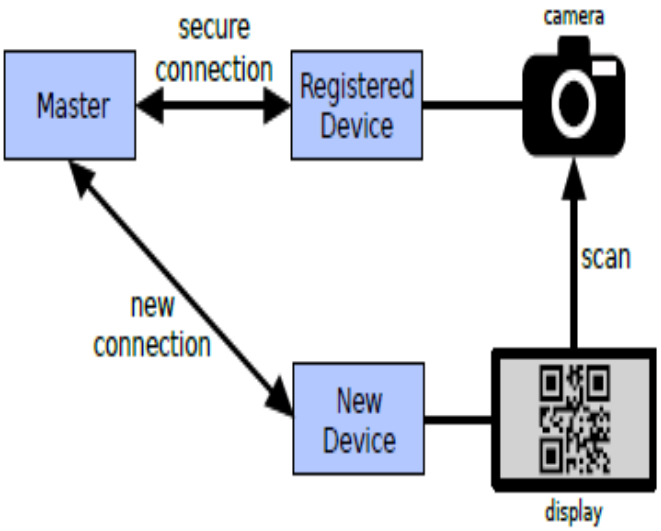

Figure 3: Passive Scenario

Tuhin Borgohain and Amardeep Borgohain [5] explains about open standard authorization and authentication (OAuth) over simple authentication and security layer (SASL) framework. This framework granting the third party applications in a limited and the resource owner grants the permission to access the application and the server resources. During permission for protected resources, the user has to request over OAuth 2.0 protocol.

S. Sridhar and Dr S. Smys[9], proposed an idea which implements the asymmetric end encryption to share the session key between the nodes and devices. The session key is also used for data transfer which will protect from the quantum attacks and denial of service (DoS) attacks.

Vaidhyesh P S and Mukund W N [10] proposed a QR code verification mechanism in order to verify the device and to get the services of an IoT device. This application will generate a QR code and encryption parameters and that parameters is used to decode the generated QR code. This mechanism is used to communicate securely with the help of signature scheme which integrates the QR code verification process.

3. Proposed System

The proposed architecture to provide the security with the multifactor authentication is designed as below Fig: 4.

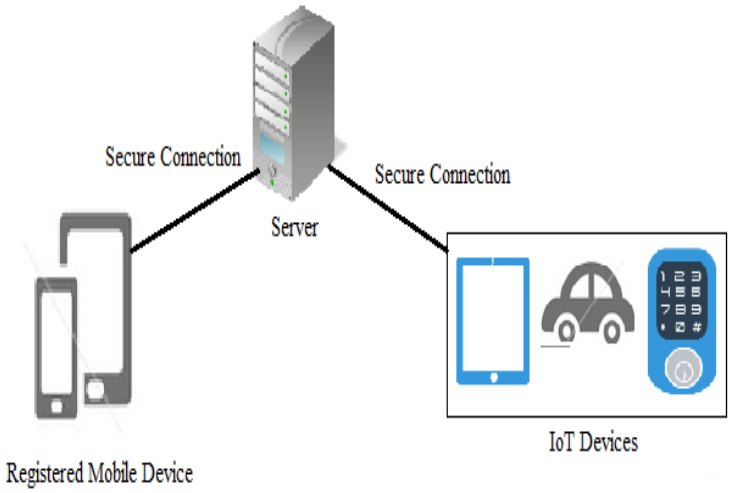

Figure 4: Proposed Architecture

In IoT environment, all the devices are controlled by the registered mobile device. In order, to security for the application the registered device have to authorize before controlling the device. To verify the user and registered device will follow the below algorithm.

Algorithm:

Step i: When user opened the controller app to control the devices. Initially it will look for authentication.

Step ii: After authentication, Server will request the device parameters like device ID and device specifications.

Step iii: Server will generate the key pair(ID(d), P) where ID(d) is a device id which act as private key and P is a public key.

Step iv: Server will encrypt the QR code i.e.,E(M,ID(d)) Where E represents encryption process, M is QR code and generates the Encypted QR Code(EQR) to user.

Step v: IoT device will scans the EQR code and decrypt with the public key P i.e., D(C,P) where C is encrypted QR Code and D is a decryption process.

Step vi: If it validates then user will get the control of devices. Otherwise user can't access the device.

The proposed system uses a public key cyptographic algorithm which are any light weighted cryptographic algorithms[11].

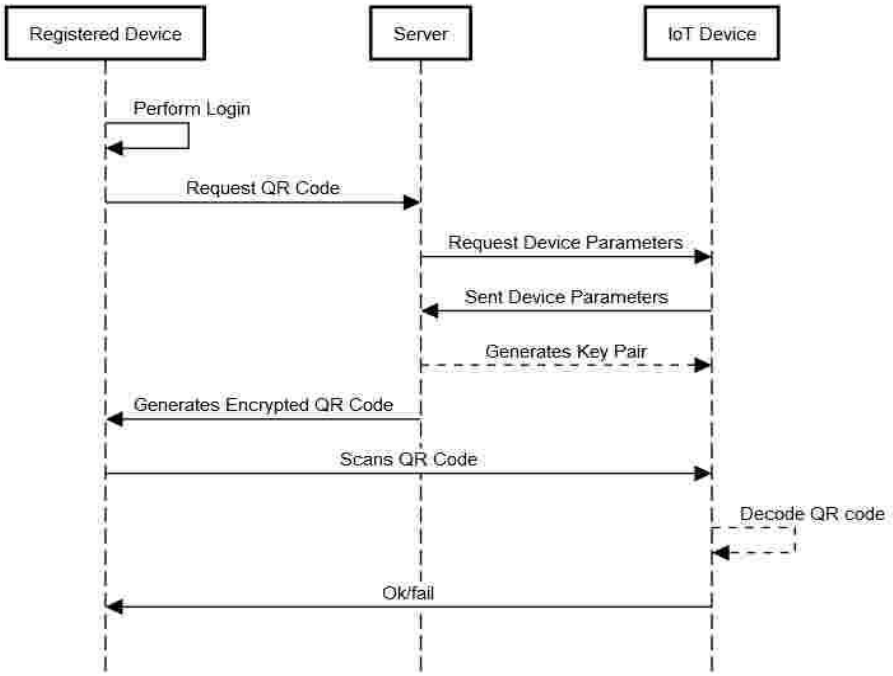

Figure 5: Work flow of the proposed system

The above Fig: 5 represents the work flow of the proposed system. Initially the user will perform login operation with the registered device. As proposed system contains multifactor authentication the encrypted QR code will be generated to the registered device. The QR code will matches by the IoT device when it decodes and got the original code from the server.

4. Conclusion

In this paper, it has been proposed that IoT Devices can controlled and communicated securely with the help of multifactor authentication uses QR code verification mechanism. This model is planned to provide the security for the application inorder to avoid the gaining access of a device. In future, this model can be extend by means of a colur QR code to

provide more security and also it can provide to security for small devices like baby monitor, coffee maker machine etc. In future if this model is implemented with the improved color QR code then it will be more secure in the multiple layers.

References

1. R. Vignesh, A. Samydurai, Security on Internet of Things (IOT) with Challenges and Countermeasures, IJEDR 2017, Volume 5, Issue 1, ISSN: 2321-9939
2. Hamoud M. Aldosari, A Proposed Security Layer for the Internet of Things Communication Reference Model, International Conference on Communication, Management and Information Technology (ICCMIT 2015), Procedia Computer Science 65 (2015) 95 – 98\
3. Tobias Marktscheffel, Wolfram Gottschlich, Wolfgang Popp, Philemon Werli, Simon Dominik Fink, Arne Bilzhause, Hermann de Meer, QR Code Based Mutual Authentication Protocol for Internet of Things, European Union, 2016, 978-1-4799-8461-9
4. "Controlling vehicle features of nissan leafs across the globe via vulnerable apis." http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html. Accessed: 2016-01-03.
5. Tuhin Borgohain, Amardeep Borgohain, Uday Kumar and Sugata Sanyal, Authentication Systems in Internet of Things, arxiv,2015
6. Sumit Tiwari, An Introduction To QR Code Technology, International Conference on Information Technology, 2016, 978-1-5090-3584-7.
7. Kinjal H. Pandya, Hiren J. Galiyawala, A Survey on QR Codes: in context of Research and Application, International Journal of Emerging Technology and Advanced Engineering, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014, ISSN 2250-2459.
8. QR Code Tutorial, http://www.thonky.com/qr-code-tutorial/
9. S. Sridhar, S. Smys, Intelligent Security Framework for IoT Devices, Cryptography based End -To- End security Architecture, International Conference on Inventive Systems and Control (ICISC-2017), 2017, 978-1-5090-4715-4.
10. Vaidhyesh P S, Mukund W N, SECURING IoT DEVICES BY GENERATING QR CODES, International Journal of Pure and Applied Mathematics, Volume 119 No. 12 2018, 13743-13749, ISSN: 1314-3395.
11. Shyamala C. K., NHarini, and Padmanabhan, T. R., "Arithmetic on Elliptic Curves Over Finite Fields", National Conference on Advanced Computing Technologies, ACT '08. pp. 25-26, 2008.