National College of Ireland

Approach to secure access of Internet of Things (IoT) using Federated Identity Management (FIM) Technology

MSc Internship
Cyber Security

Prem Ananth Raj Sundararajan
Student ID: x19143095

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name	Prem Ananth Raj Sundararajan
Student ID	x19143095
Programme	Cyber Security
Year	2020
Module	MSc Internship
Supervisor	Vikas Sahni
Submission Due Date	17-08-2020
Project Title	Approach to secure access of Internet of Things (IoT) using Federated Identity Management (FIM) Technology
Word Count	5581
Page Count	19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature	Prem Ananth Raj Sundararajan
Date	16-08-2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Approach to secure access of Internet of Things (IoT) using Federated Identity Management (FIM) Technology.

Prem Ananth Raj Sundararajan
x19143095

Abstract

In today's timeline Internet of Things (IoT) is one of the fast-emerging and versatile technology. They are readily available for access from any part of the world, and they play a crucial role in combining existing home appliance and the internet. The challenge faced in this technology is ensuring the access of IoT devices over the internet using safe and secure procedures. Numerous threats can cause harm to an IoT device or the environment hosting it. In this paper, the aspect of secure access of IoT device over an infrastructure across the internet is focused. An application is designed by following the principles of Federated identity management (FIM) approach for secure access of any IoT devices over a network. After careful research of numerous ideas and published works, we have designed and implemented an application that uses JSON Web Token (JWT) for authentication and showcases greater time efficiency and exerts less computation stress on the IoT devices. An experiment has been performed to compare this with existing research and algorithm. Thus, ensuring faster access to IoT devices over the internet.

1 Introduction

The aspect of the Internet of Things (IoT) has given a new horizon to the current technological world. With the increase in the compatibility of Internet of Things (IoT) and its approach over scalability has aided the transformation from regular homes to smart homes. The design of any smart home is based on the usage of various switches and sensors for any household purpose that include lighting, heating and other fundamental aspects that are required, and they can be controlled remotely [1]. The idea of any smart home is to bring the advantage of remote operation and monitoring of these devices using the internet. The aspect of automation of a typical home is driven by introducing IoT that makes it a growing smart home. Combining an IoT device with smart home technology is the prime factor that will increase the level of automation in any household.

The probability of any IoT device to become a possible target to any threat in the cyberspace is more as there is a rise in access to information. With confidence and the use of data, systems, applications, and users, the aspect of defence, safety and financial efficiency are being advanced in the IoT environment. However, the element of protecting any IoT devices from various cyber threats remains. The critical features in ensuring the safety of an IoT device or infrastructure based on the type of authentication, user identification and the necessary protocols. However, there remains a challenge till date that many IoT devices are not built with the required capability that makes them expedite the aspect of performing the extensive computation, storing and to function using new protocols for authentication that are based on any specific algorithms.

1.1 Identity and Access Management

The key challenge when implementing cryptography is the aspect of handling critical problems. The broader approach of today's systems has its focus on the specific cryptographic algorithm, and all of them use a specified key, which has to be safeguarded for all the client who uses that system. For the identity and access management application, the key needs to satisfy the criteria of creation, updating, delivery and destroying, ensuring that the identities of the key can be verified by all the individuals who have access to it. This application provides control of the devices that are safely connected.

On the contrary managing of the devices and ensuring that level of confidentiality in the IoT environment highlights newer issues. There are three categories in the IoT architecture namely perceptual, network, and application. We focus on the application layer as it has the responsibility of ensuring there is communication between the IoT device and the end users and also it collects the necessary data required for the users. Thus, a proper identity and access management is to be implemented.

1.2 Authentication of IoT

The authentication element is for identification of every IoT device. It includes establishing trust and connections between a system and the end user. The end users have to provide the required credentials (password or token) for the authentication and at times if they are misplaced it can be misused. Let us examine an instance in which we authenticate a service, the point of focus in on the service but device or where it is deployed. The firm that deploys these systems have to ensure not only the necessary credentials are given for the service to function however it also needs to be checked of its integrity of its operation that will result in safe access of the system.

This report has been sectioned into Related works, Research methodology, Design Specification, Implementation and Evaluation. We have described the functioning of the traditional authentication scheme versus the modern ones. A comparison has been depicted by building an application to manage IoT devices that is designed by following the principles of Federated Identity Management that is implemented by using traditional token based versus JSON token based authorization that will result in faster and safer access of any IoT device over the internet.

1.3 Research Question

Can Federated Identity Management (FIM) technology be an identity management solution for faster access to Internet-of-Things (IoT) by using Json token?

- Implementing a token-based authentication system, using an application that showcases faster access to Internet-of-Things (IoT) devices

2 Related Work

This section showcases a detailed overview of the related papers that use various technologies. Based on numerous papers that have been published, most of the authors have proposed a variety of methods from the implementation of authentication and authorization, the aspect of using different kinds of encryptions, frameworks, protocols with the aid of machine learning algorithms, and also use of implementing blockchain method has showcased based on the accuracy and time taken for execution of the algorithm have been discussed below in detail.

2.1 Encryptions based Research.

Lee et al. [2] presented an idea of for IoT devices based on lightweight authentication protocol on symmetric XOR encryption. The authors in this paper focused on the symmetric encryption schemes that were of lightweight and eliminated asymmetric encryption that was heavyweight, resulting in this protocol being highly constrained on the computation aspect for IoT devices. Anggorojati et al. [3] used a lightweight threshold cryptographic based Group Authentication (TCGA) approach h that ensured security and scalability. This approach performs an identity checks on all the IoT devices, thus resulting in minimum resource usage and power consumption, on the contrary, it faced a drawback in implementation over clusters.

P. Porambage et al. [4] developed an enhanced IoT authentication scheme that is based on asymmetric cryptography-based authentication that can be used for improving the authentication performance. However, it resulted in causing more vulnerability to the IoT environment that used the virtual authentication credentials. V L Shivraj et al. [5] showcases the use of an Elliptic Curve Cryptography scheme with the integration of Lamport's OTP algorithm that makes is secure. The drawback in this approach is the implementation of a sizeable cryptographic scheme on an IoT device, which has less computation capability that is not efficient. Nan Li et al. [6] using a public-key encryption scheme proposed a lightweight authentication protocol for IoT application; however, this was an application-based solution that required high computational input. However, it lacked secure, lightweight multifactor authentication techniques. The limitation here was that it had a single point of failure and lightweight authentication was more prone to cyber-attacks.

2.2 Framework and Protocol based Research

Nehme et al. [7] focus on the data authentication framework of IoT. The data processed in these are served as streams that have punctuations-based security, that are analysed before the client receives the data. Thus, these aspects do not apply on any security rules such as Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Mandatory Access Control (MAC) can be implemented as solutions. However, concern raises on the security rules that can be duplicated, and the level of consistency drops over different IoT devices in the infrastructure. Chen et al. [8] devised an idea to secure Industrial IoT Objects by developing a framework based on authorization using annotated metadata. The orientation aids processing large data and focuses on multiple dimensions and also ensured to maintain its efficiency in the authorization to keep on par with the requirements for any security of the IoT devices. The drawback was it required a considerable computation power that is a limitation in the IoT environment. Zhang et al. [9] portrayed a disturbed access control in a network that ensured the aspect pf preserving privacy. It was a token-based approach with a multiuser network approach and used to central token distributing authority that protected user privacy. This could not solve the structuring of access control policies. S. Cirani et al. [10] described a technique where the authorization layer can destroy any service hosted by the IoT device without

implementing the standard OAuth technique, however an external authorization service named IoT-OAS performed this action. Thus, making it vulnerable when deployed in a large infrastructure.

M. Noureddine et al. [11] proposed a scheme based Oauth 2.0 that is optimized by decreasing the authentication requests that are not necessary by not affecting the primary security requirements thus mitigating threats such as denial of service (DoS) and distributed DoS (DDoS) .T. Dierks et al. [12] proposed an application based on OAuth authorization framework that enabled secure access to the transport layer in a network device that could be connected to the IoT devices that could prevent tampering and eavesdropping of data. However, this was application-oriented and was not implemented on the IoT devices instead of on the network device connected to it, thus resulting in making the IoT devices vulnerable. F. Yang et al. [13] focused on the OAuth 2.0 protocol vulnerabilities and developed analysis and studied the root cause of common attacks such as impersonation attacks, replay attacks, and Cross-site request forgery attacks. M. Alshahrani et al. [14] designed a lightweight authentication framework model that uses Dynamic identities and using temporary keys of IoT nodes. By using Modular Network Testbed, the framework was successfully implemented; however, this could not completely prevent DoS and DDoS attacks.

Jing Liu et al. [15] focused on a key establishment that is based on Elliptic Curve Cryptosystem(ECC) algorithm that uses role-based access control authorization method for accessing the IoT device; however, this algorithm does not provide encryption that is of direct approach; instead, a key pair generation has to be manually performed. Seitz et al. [16] proposed a framework in which a Trusted Third-Party entity acts as an Authorization Engine. This helps in solving requests for a user that needs to access any of devices data or service for authorization that are restricted. It is designed for facing Rest API; thus, any IoT device can access them. It has the drawback of a complex framework that results in no trust being established between devices. Kothmayr et al. [17] highlights using Datagram Transport Layer Security protocol by designing a two-way authentication approach for access to IoT devices. The proposed method showcases the protocol used between point to point communication but lacks the focus on administration and management of many devices in a single instance.

M. N. Aman et al. [18] designed a mutual authentication protocol that is light-weighted and could be implemented on IoT devices. This method was efficient in the aspects of computation, memory, and deployment. However, the use of this approach had an issue with the timing aspect as it reduced the latency of authentication that was dues to decrease in my number of messages that were to be exchanged between different IoT devices. Karlof et al. [19] proposed a secure routing authentication method in an IoT network that could prevent any threats and ensure a mechanism to safeguard. However, the aspect of resource constraint was again based on low computational and processing capability.

2.3 Blockchain methodology and Machine Learning based Research

Miettinen et al. [20] analysed the packet header of any connecting devices to the IoT devices that were formalized using a passive fingerprinting approach. Random Forest single classifier approach was followed to identify and authenticate the device. The limitation with this approach was that it was unable to identify the instance of the device of the multiple devices of the same model or vendor types. Y. Rahulamathavan et al. [21] researched a method to focus on the challenges of authentication by developing a framework using blockchain technology to ensure privacy on IoT application by building upon the mechanism of attribute-based

encryption. The challenge that it faced was it had high risks when implanted in the cluster infrastructure or on a group network, thus making it a non-viable solution.

N. Kshetri .[22] provided an overview of blockchain technology for IoT technology, and addressed the security challenges over IoT network, it described the aspect of lacking a basic architecture, limited availability of cloud resource and the possibility of data manipulation and other various limitation aspects concerning to compute, storage and costs. M. A. Rashid et al. [23] designed a model based on blockchain technology that can be deployed over a network via a multi-layered architecture. The author has used Genetic Algorithm to device this model. This also focuses on device-level authorization elevating the security features. However, the data set required for using Genetic algorithm is vast that results in more values to be used for operation making in less viable.

2.4 Key Researches

H. Kim et al.[24] described a model that emphasizes the aspect authentication and authorization based on the mechanism of key distribution over a network that ensures more security for IoT devices by overcoming the access mechanism that are traditionally certificate-based.

R. Moosavi et al. [25] proposed an architecture based on authentication that relies on a certificate based DTLS (Datagram Transport Layer Security) handshake protocol that ensures a solution for safe access of IoT devices. It also showcases the better time efficiency based on the access to the devices.

L. Seitz et al. [26] showcases a framework that is flexible and uses the concept of authorization engine and extensible Access Control Markup Language (XACML) for processing the authorization handshake successfully. The aspect of time efficiency is made better by using these papers as a baseline for the proposed model.

Based on the flexibility of different theories and algorithms, understanding the various methods based on their attributes and the functionalities. An appropriate approach is required to be implemented for greater time efficiency of the authentication methodology and ensure the secure access of the IoT device over deployed infrastructure. From the above discussion, a conclusion has been reached to focus on Oauth 2 implementation using JSON token, and this has been discussed in the further section.

3 Research Methodology

The critical aspect of the above papers is about the different methodologies that are utilized for safe and faster access to IoT devices or infrastructure. The key researches section has been selected based on authentication and authorization to an IoT device or environment. The criteria of selection are based on specific attributes as described below.

[24] Describes the attribute of key distribution over a network that has IoT devices deployed in them. In this paper the concept of generation of a key for every authentication request that results in a greater level of security. The architecture design addresses the aspects of IoT Security, overcoming the resource constraints and also the slow rate of overhead responses that are slower than the standard SSL/TLS bases connections.

[25] Depicts the attribute of the certificate-based protocol being used for the authentication request that showcases fast access to the IoT device or environment. The design architecture centralized based as it uses key management scheme between the gateway and the sensor nodes. It also focuses on the mitigation of DoS attack with its distributed architecture.

[26] Focuses on the attribute of authorization engine in which the use of XACML showcase the fast and secure execution of authentication request. The framework design showcases methods to distribute the resources between devices that are more constrained versus the less constrained while ensuring that the messages are minimum to the constrained devices.

Based on these attributes mentioned above an application has been designed and implemented that manages IoT devices or infrastructure which uses the principles of Federated Identity Management, OpenID and OAuth 2. It also uses the concept of JSON tokens for performing faster execution of authentication request of any user into the IoT management application. A simple description of the mentioned technologies has been showcased below.

3.1 Federated Identity Management (FIM)

The establishment of trust between an Identity provider and service provider is performed by signing up contracts for data processing which is managed by the Federated Identity. The identity services among any users and the IoT devices are managed by the identity and the service provider using a management application and also should ensure that all have the aspect of trust [27]. The Federated Identity management will be the focus of OpenID for authentication and OAuth 2 for authorization.
.

3.2 OpenID

It is a cluster of protocols that are based on identity and is defined with a format identifier which is used for transmission of information. Considering a user identity which can be used for accessing various application where the user need not enter the password multiple time, as the identity provider validates the session for the server to gain access to control. This protocol is more focused on the aspect of authentication.

3.3 OAuth 2

OAuth 2 is a type of protocol that is primely focused on the authorization. The communication between users and any IoT resources is primarily based on specifically designed application programming interface (API). OAuth 2 has a primary function is to connect users to their request by fetching passwords that are entered initially under OpenID. It needs to identify the user whenever a request is made. A vulnerability arises as a pattern can be developed for every request. OAuth defends such kind of vulnerability by creating a secure architecture that policy-driven, flexible and safe.

Based on the key researches studied in section 2, the research [26] mainly showcases the aspect the identity key had to be specified whenever access is required by the user to login to the IoT device and perform any action. An identity key is represented by a string of characters that is provided to the end-user in an organisation. Every time an end-user has to provide the identity key to access the IoT device. This step is time-consuming as the response time is slow when a large number of devices are in the infrastructure. Also, the integrity of the key could be easily compromised, thus making the IoT device slower to access and making it vulnerable.

By implementing the solution specified on the research [26] for improving the response time and designing a secure approach other than the key-based [24] and certificate-based [25] that can mitigate the aspect of integrity. With the limitation of showcasing a large scale IoT network, the research[26] has been implemented in a simpler form(hard token-based approach) in this paper that acted as a baseline for the proposed solution. An application was developed that uses JSON tokens which are generated and validated, that result in faster response time to access the IoT device over the network.

3.4 Performance Metrics

This paper will showcase the performance of the algorithm that can be analysed based on the token types and memory usage of the IoT devices.

Token type: The use of hardcoded token and JSON Web Token (JWT) and can be identified depending token type based on the request versus the response, respectively.

Time taken: The time taken for the client to complete an authentication request.

4 Design Specification

The below model Fig.1. showcases the workflow of authentication and authorization:

•The primary setup is to create an account that is performed by the end-user
•The end-users then request for a token from the provider
•The device validates and then authenticates by using the generated JSON token that performs a secure communication
•The communication received by the IoT device is verified by the provider based on the roles and the identity that is assigned by the administrator
•The identity of the IoT devices can be centrally managed by the identity provider. New or existing devices can be added or removed from the inventory respectively

The approach of identity provider showcases as a central repository that results in building a trusted environment between the identity provider and the IoT devices, as there no trust created at the initial integration and the trust is established only after a successful completed of a request. If in case an IoT device is under attack, it can be isolated or removed from the inventory without affecting the infrastructure. Monitoring the IoT devices at any point in time is also easier using this management application. The aspect of JSON token that is generated by the provided has to be time centring. Short time validity of token is set up over the long duration as it is more secure, and it also mitigates the pattern learning attack techniques.

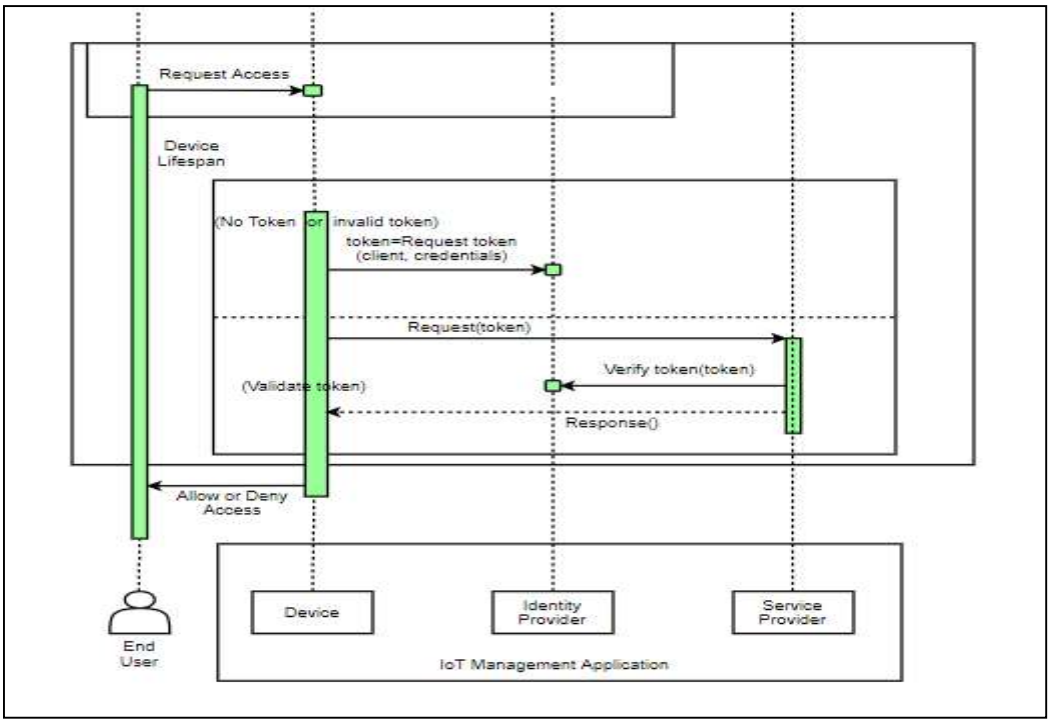

Fig.1.

Once the IoT management application is configured, OAuth 2 protocol is used as the bearer token, and the verification issued is of the type JWT. There are many advantages to this approach as it can carry more information such as credentials and user role. As it can be managed from a central identity provider making it lighter, easier to manage the access of IoT devices.

5 Implementation

The implementation of the proposed solution has been developed by building an application. The application will showcase both the existing approach and the proposed approach. That will ensure that a comparative study has been performed. The results are tabulated and graphically represented.

The initial step is to build the application for the designer of the model, .NET framework, and C# programming language has been used to develop IoT device management application. HTML and jQuery have been used for developing the front-end user interface. Microsoft SQL Server has been used for deploying the database.

A client-server architecture is used to showcase the communication between an end-user and IoT devices using a management console. Once the setup is built; the necessary experiments are conducted. In order to understand the proposed solution that is token-based, postman [28] tool is used for further analysis, and it is used for studying the behaviour of the token in this scenario. The approach has been categorised into two sections first being the hard token type for the existing approach and the second being JSON token type for the proposed solution has been showcased below.

5.1 Existing Approach

Based on the research performed for the existing approach to understand the time efficiency of the hard token, an application has been built. The login page has been showcased wherein the users need to input their credentials. If a new user needs to sign up, they have to register themselves using the "Register Here" option. Once the user has successfully registered, they can log in to their profile, as shown in Fig.2.

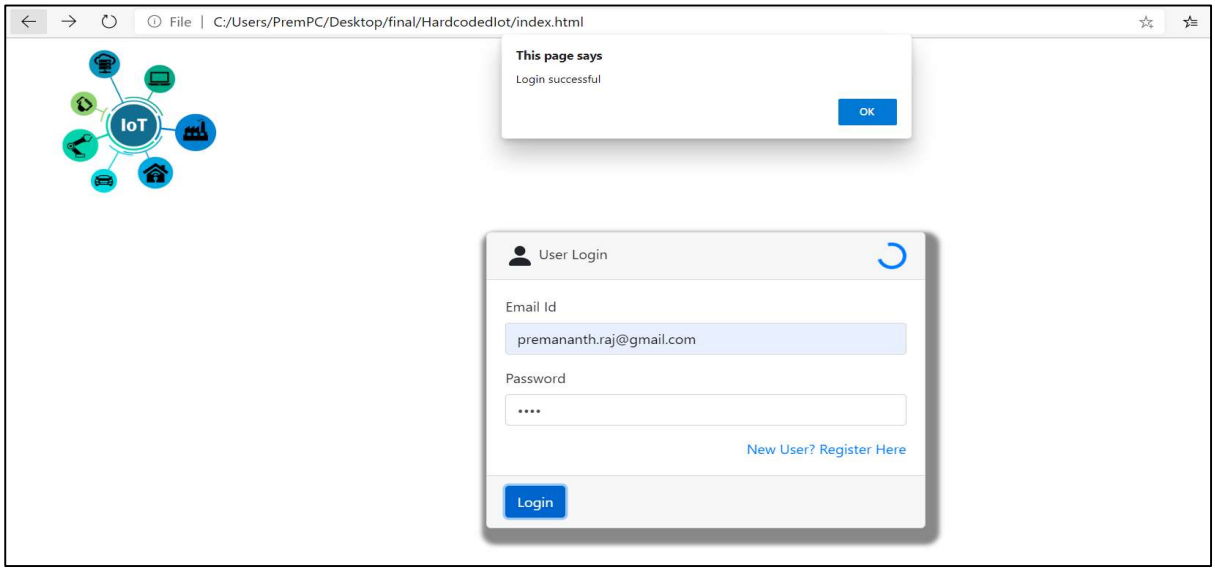

Fig.2.

For access to an IoT device, the user needs to enter the device Id to control the IoT device. The Device id is a unique identifier which is device-specific, and it is hardcoded to the IoT device. User will not be able to gain access to their account without specifying the correct Device id shown as per Fig.3.

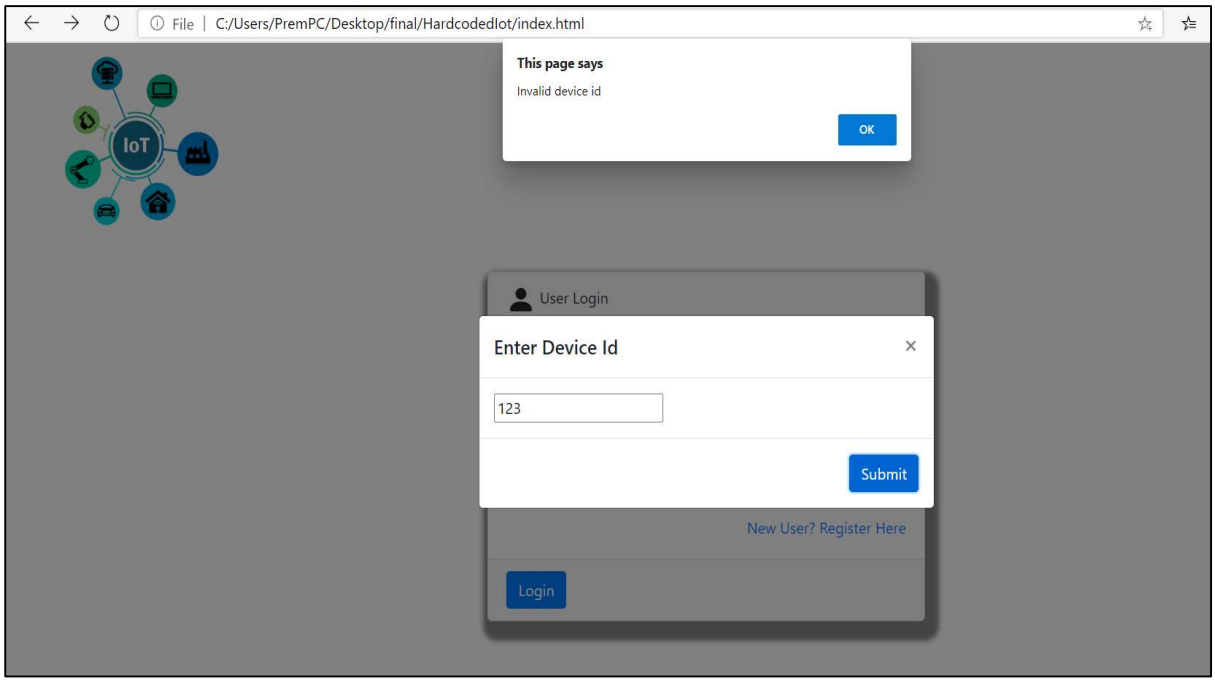

Fig.3.

Once a successful login, the user can control the IoT device. The time taken to access the console has been calculated for the existing scenario in Fig.4.

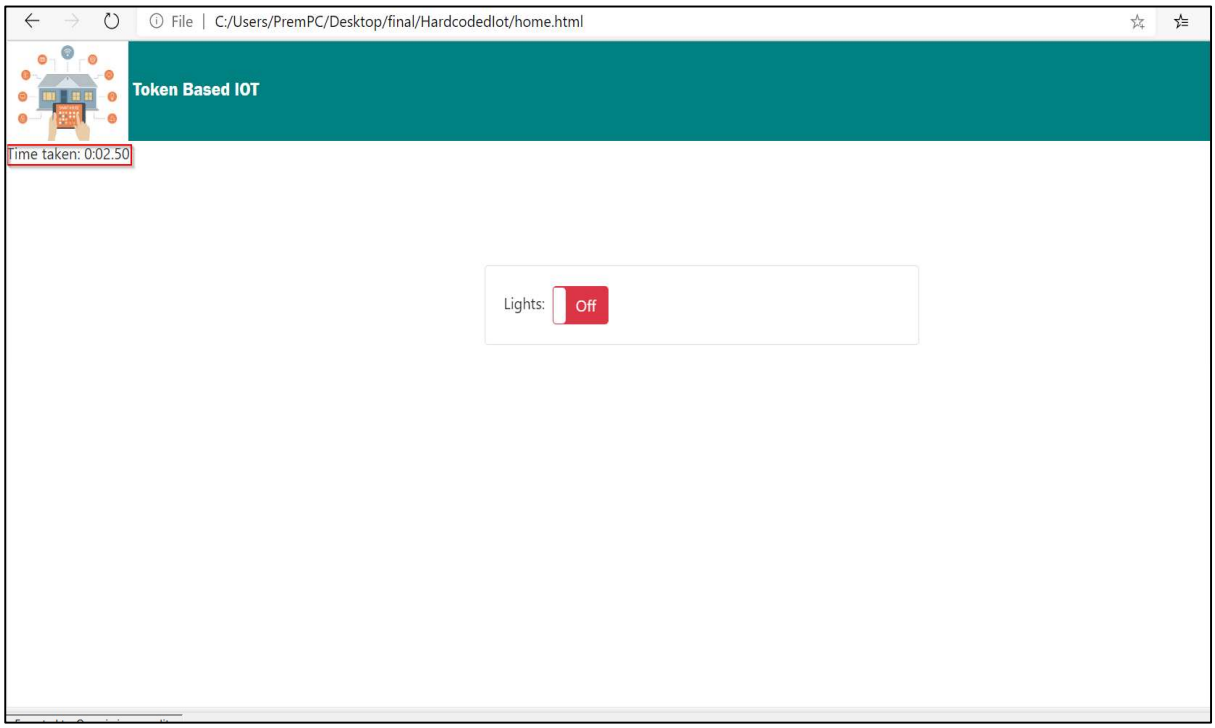

Fig.4.

The feature of session timeout is designed based on the existing approach to ensure session validation, as shown in Fig.5.

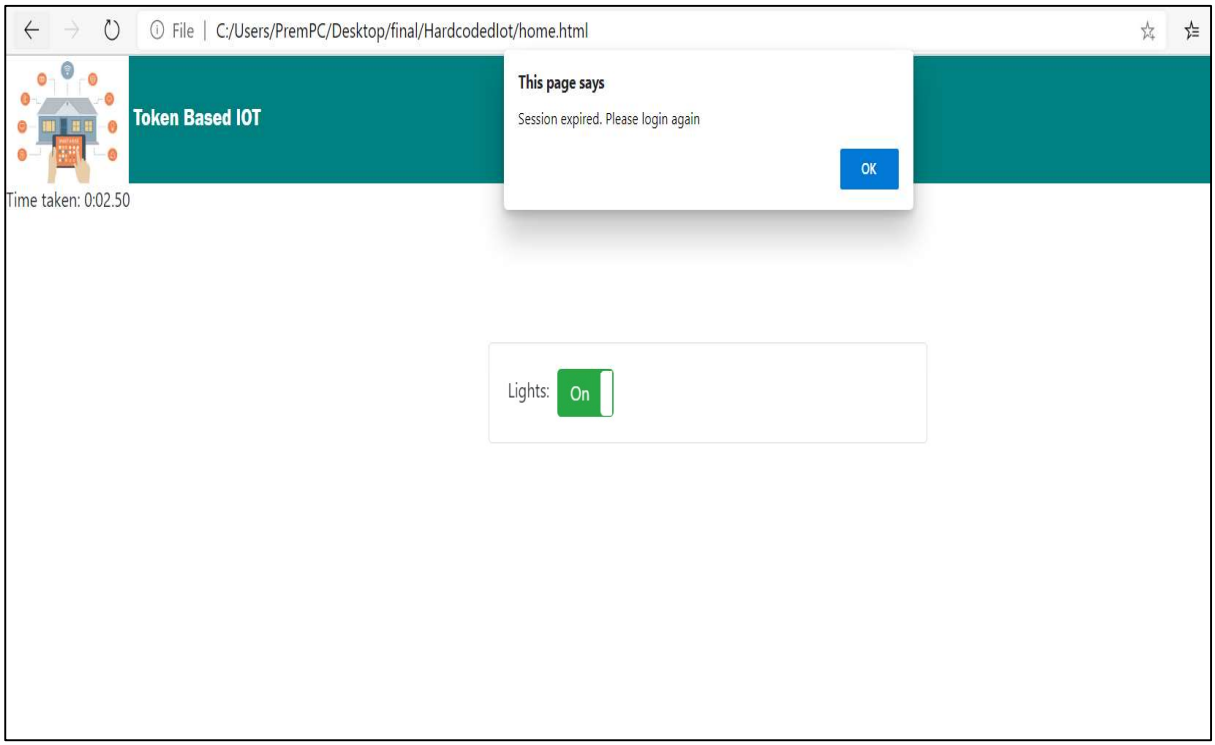

Fig.5.

5.2 Proposed Approach

The proposed solution for the research question is shown through an application. The login page in similar to the existing approach that showcases wherein users need to log in. If a new user needs to sign up, they have to register themselves using the “Register Here” option. Once successfully logged in, the user will be able to power on or off the devices. In this approach, all the IoT devices are mapped into the user’s profile, as shown in Fig.12.

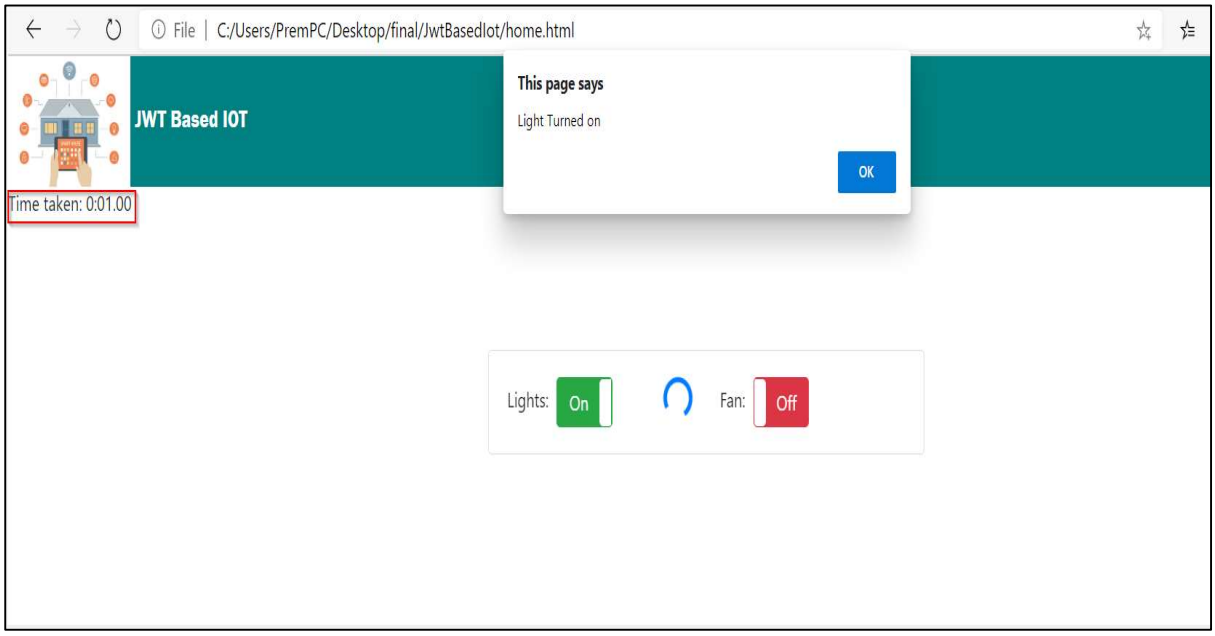

Fig.6.

The aspect of unauthorized user error is shown when the token validity expires. Hence the user has to re-login to control the IoT device; this is done to ensure a new token is generated every time for faster and safe access to the device as shown in Fig.7.

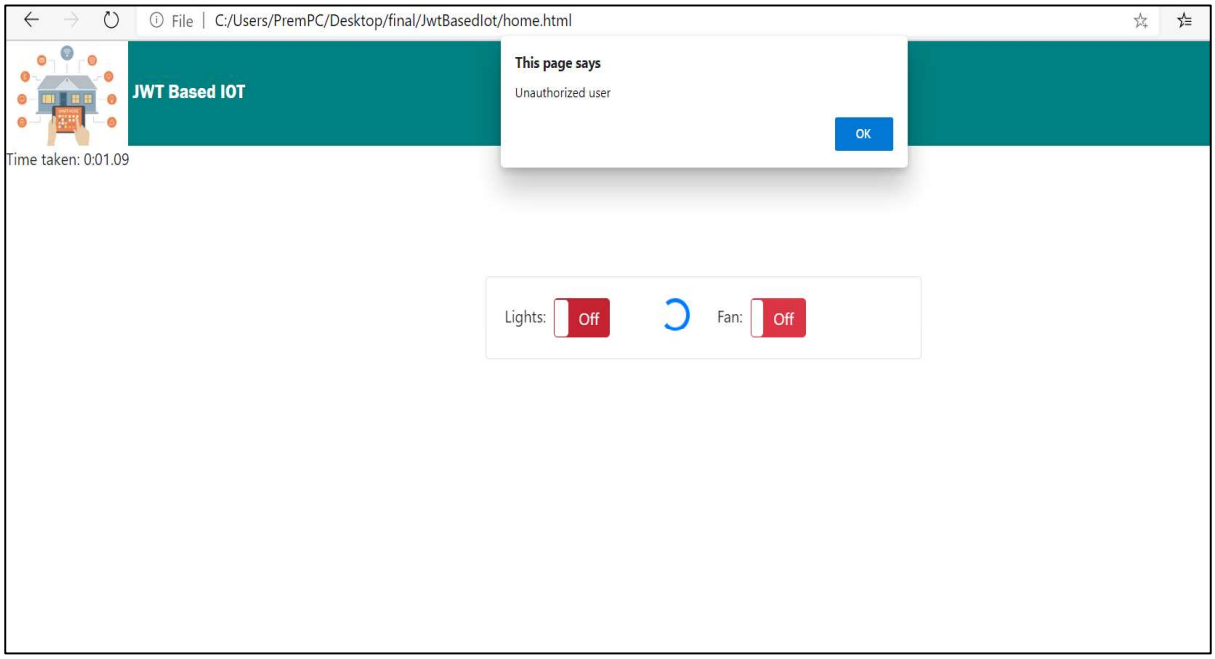

Fig.7.

Using the Postman [28] tool, the user's credential is parsed, and the result showcases the token format, which is the JSON type. The time taken for the completion of the request and the message of success or failure has been shown in Fig.8.

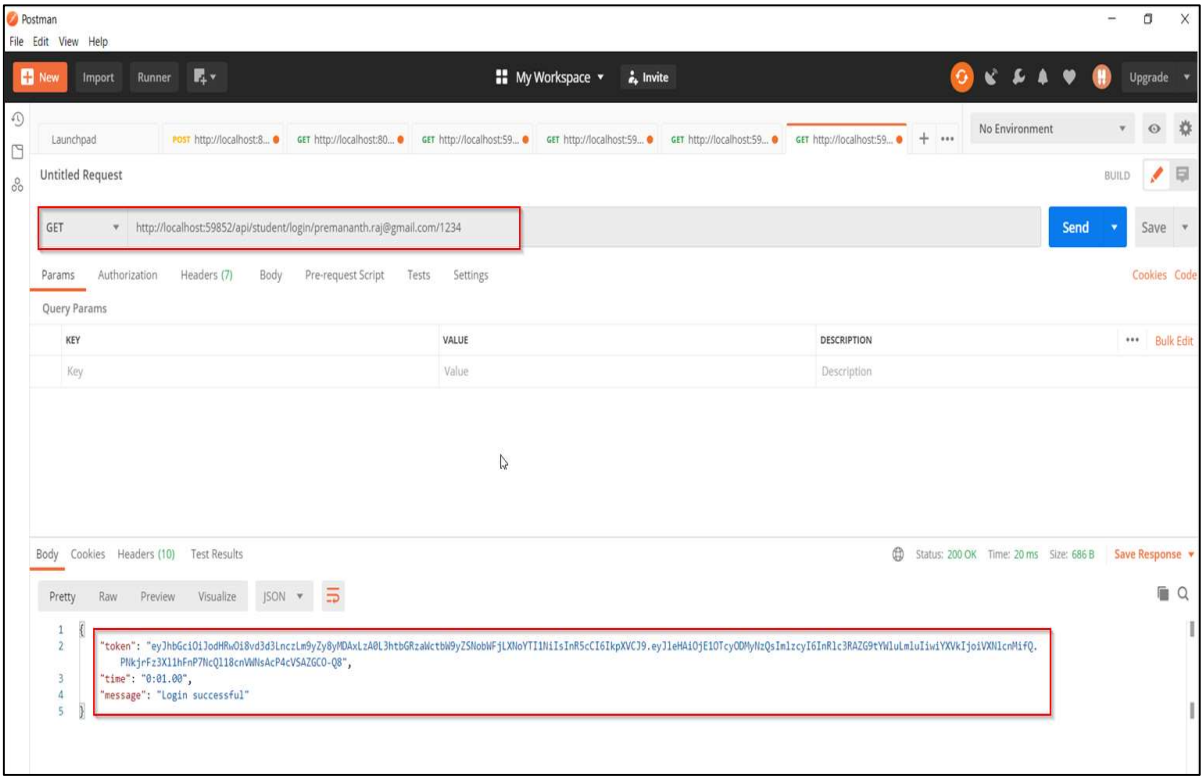

Fig.8.

If an incorrect credential is provided, then the token and time fields are empty, with an error message showcased as shown in Fig.9.

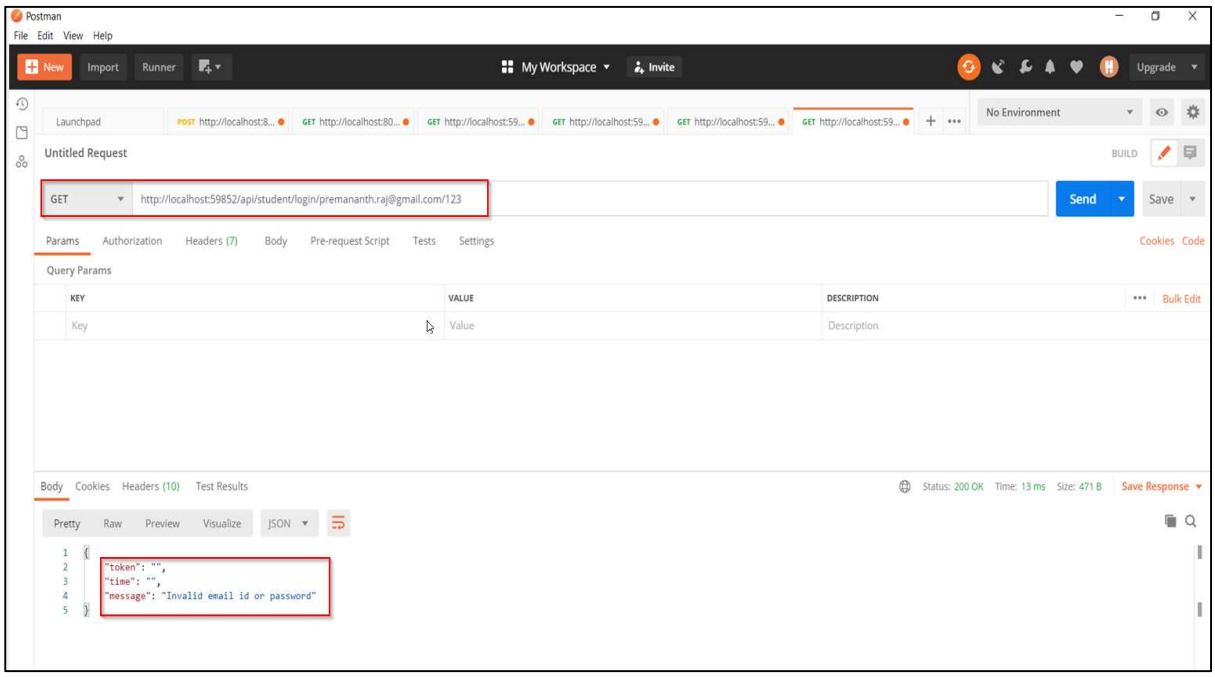

Fig.9.

6 Evaluation

Based on the proposed model, the experiment is performed to calculate the time efficiency by using hard token approach versus the JSON token approach. The process is recursively performed in order to calculate accurate results. The related researching based on other algorithms are highlighted in the research methodology section. The experiment is based on a user accessing an IoT device using the IoT application. Thus, the following results have been gathered.

6.1 Experiment 1

When using the hard token approach, the time taken for the request to complete is shown in Fig.10.

Requests	Time Taken(ms).
1	250
2	260
3	255
4	310

Fig.10.

6.2 Experiment 2

When using the JSON token approach, the time taken for the request to complete is shown in Fig.11.

Requests	Time Taken(ms).
1	100
2	115
3	125
4	127

Fig.11.

The average time has been calculated for Hardtoken and JSON token from the above experiment is shown in Fig.10.

Token Type	Hardtoken	JSON token
Average Time(ms)	278.25	113.5

Fig.12.

Comparing the results of request time of the existing and the proposed approach and the average time have been graphically representation has been showcased in Fig.12. and Fig.13.

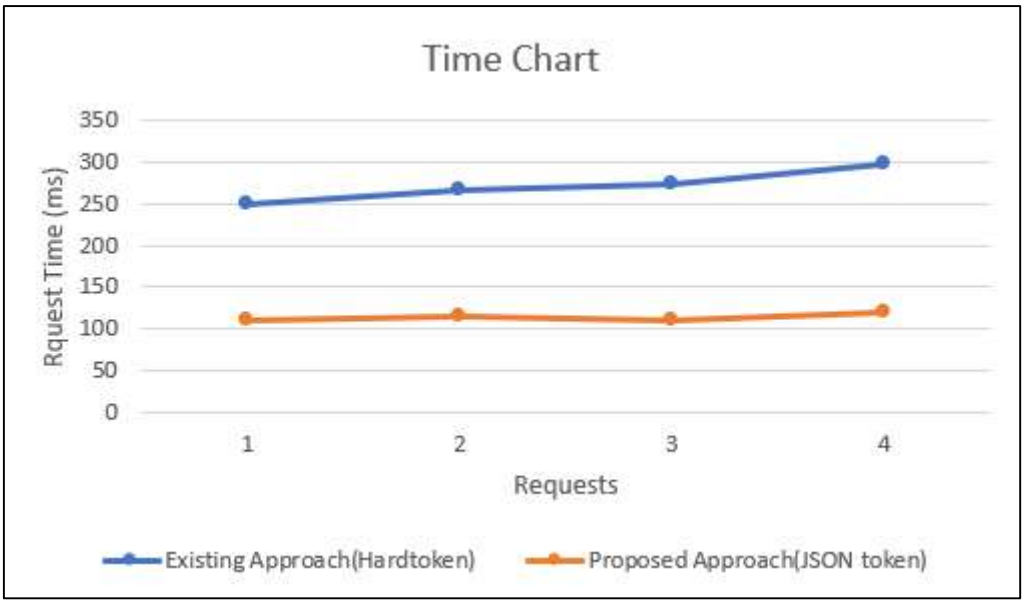

Fig.12.

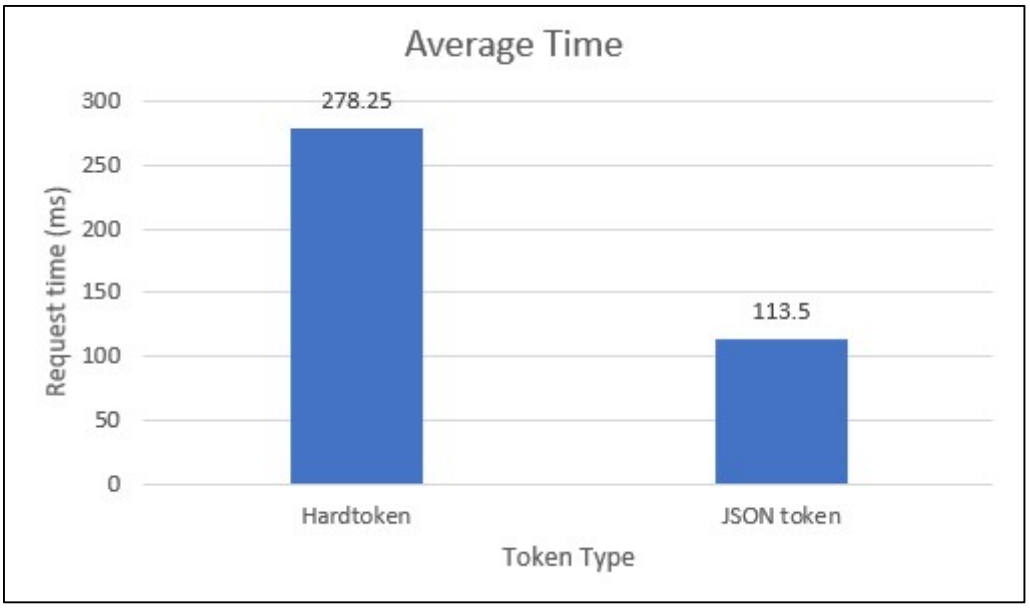

Fig.13.

6.3 Discussion

Based on the solution implemented and the produced results for the goal of this study, the research question that is mentioned in section 2 with objectives have been successfully answered and the results obtained have been reasonable. Based on the calculated average shown in Fig.3. it indicates that the JSON token approach completes a request faster when compared to the hard token approach. The designed and implemented model showcase greater time efficiencies based on the request time completion, thus making it a viable method that can be used. In addition, this project may face challenges in managing a large number of IoT devices in real-time.

7 Conclusion and Future Work

This paper presents a safer and time-efficient authentication methodology to access an IoT device or environment using an IoT management application. Furthermore, detailed research has been carried out to understand the various algorithms used in the existing methodologies and bring in newer and efficient methods to enhance the access capability of IoT devices over the internet. An attempt to showcase the comparison between an existing authentication model and proposed model has been showcased better time efficiency, i.e. faster execution time. A method that is faster and safer is more preferred in today's timeline.

The experimental conducted showcase results in an approximate measure of the response time of the existing model as well as the newly developed model that executes faster, which is useful for large infrastructure. Thus, making it a more efficient and desired model in managing larger IoT environment. Future work can be performed by adding encryption algorithms for on request/response headers along with token-based authorisation to enhance security and time efficiency.

References

[1] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, and Saleem Ullah. 2017. Security issues in the internet of things (iot): a comprehensive study. International Journal of Advanced Computer Science and Applications (IJACSA), 8, 8.

[2] J. Lee, J. H. Chang and D. H. Lee, "Security flaw of authentication scheme with anonymity for wireless communications," in IEEE Communications Letters, vol. 13, no. 5, pp. 292-293, May 2009.

[3] Neeli Rashmi Prasad Bayu Anggorojati Parikshit Narendra Mahalle and Ramjee Prasad. 2012. Capability-based access control delegation model on the federated iot network. In The 15th International Symposium on Wireless Personal Multimedia Communications. IEEE, Taipei, Taiwan, 604608.

[4] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, 2014, pp. 2728-2733, doi: 10.1109/WCNC.2014.6952860.

[5] V. L. Shivraj, M. A. Rajan, M. Singh and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, 2015, pp. 1-6, doi: 10.1109/NSITNSW.2015.7176384.

[6] Li, Liu, D, & Nepal, S. (2017). Lightweight mutual authentication for IoT and its applications. IEEE Transactions on Sustainable Computing, 2(4), 359-370.

[7] R. V. Nehme, E. A. Rundensteiner, and E. Bertino, "A security punctuation framework for enforcing access control on streaming data," in 2008 IEEE 24th International Conference on Data Engineering, April 2008, pp. 406–415.

[8] Chen, G, & Ng, W. S. (2017, November). An efficient authorization framework for securing industrial Internet of Things. In TENCON 2017-2017 IEEE Region 10 Conference (pp. 1219-1224). IEEE.

[9] R. Zhang, Y. Zhang, and K. Ren, “Distributed privacy-preserving access control in sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1427–1438, Aug 2012.

[10] S. Cirani, M. Picone, P. Gonizzi, L.Veltri, and G. Ferrari, “IoT-OAS:An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios,” IEEE Sensors Journal, vol. 15, no. 2, pp. 1224–1234 Feb. 2015.

[11] M. Noureddine and R. Bashroush, “A Provisioning Model towards OAuth 2.0 Performance Optimization”, 10th IEEE International Conference on Cybernetic Intelligent Systems, pp. 76-80, Sept. 2011.

[12] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol, RFC 5246, Network Working Group, Aug. 2008.

[13] F. Yang and S. Manoharan, "A security analysis of the OAuth protocol," 2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, 2013, pp. 271-276.

[14] M. Alshahrani, I. Traore and I. Woungang, "Design and Implementation of a Lightweight Authentication Framework for the Internet of Things (IoT)," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 2019, pp. 185-194.

[15] J. Liu, Y. Xiao and C. L. P. Chen, "Authentication and Access Control in the Internet of Things," 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, 2012, pp. 588-592, doi: 10.1109/ICDCSW.2012.23.

[16] L. Seitz, G. Selander and C. Gehrmann, "Authorization framework for the Internet-of-Things," 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, 2013, pp. 1-6, doi: 10.1109/WoWMoM.2013.6583465.

[17] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," 37th Annual IEEE Conference on Local Computer Networks - Workshops, Clearwater, FL, 2012, pp. 956-963, doi: 10.1109/LCNW.2012.6424088.

[18] M. N. Aman, K. C. Chua and B. Sikdar, "A Light-Weight Mutual Authentication Protocol for IoT Systems," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8253991.

[19] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003., Anchorage, AK, USA, 2003, pp. 113-127, doi: 10.1109/SNPA.2003.1203362.

[20] M. Miettinen, S. Marchal, I. Hafeez, T. Frassetto, N. Asokan, A. R. Sadeghi, and S. jg2511–2514, 2017.

[21] Y. Rahulamathavan, R. C. Phan, M. Rajarajan, S. Misra, and A.Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in 2017 IEEE International Conference on AdvancedNetworks and Telecommunications Systems (ANTS), 2017,pp. 1-6.

[22] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," in IT Professional, vol. 19, no. 4, pp. 68-72, 2017.

[23] M. A. Rashid and H. H. Pajooh, "A Security Framework for IoT Authentication and Authorization Based on Blockchain Technology," 2019 18th IEEE International

Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 264-271.

[24] H. Kim, A. Wasicek, B. Mehne and E. A. Lee, "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, 2016, pp. 114-122, doi: 10.1109/FiCloud.2016.24.

[25] Rahimi Moosavi, Sanaz & Nguyen gia, Tuan & Rahmani, Amir M. & Nigussie, Ethiopia & Virtanen, Seppo & Isoaho, Jouni & Tenhunen, Hannu. (2015). SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. Procedia Computer Science. 52. 10.1016/j.procs.2015.05.013.

[26] L. Seitz, G. Selander and C. Gehrmann, "Authorization framework for the Internet-of-Things," 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, 2013, pp. 1-6, doi: 10.1109/WoWMoM.2013.6583465.

[27] A. Adireddy, U. Gottapu and A. P. Aravamudhan, "Usercentric federation of access to Internet-of-Things(IoT) devices: A valet key for IoT devices," 2016 International Conference on Circuits, Controls, Communications and Computing (I4C), Bangalore, 2016, pp. 1-7.

[28] Postman.com. 2020. [online] Available at: <https://www.postman.com/downloads/> [Accessed 13 August 2020].