International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6514
***Article Received**: 20 January 2023 **Revised**: 22 February 2023 **Accepted**: 02 March 2023*

Physiological Conditions Monitoring System Based on IoT

Meena Gulati[1], Dr. Rakesh Kumar Yadav[2], Dr. Gaurav Tewari*
[1]Research Scholar, Department of Computer Science Engineering,
Maharishi University of Information Technology, Lucknow
[2]Research Supervisor, Department of Computer Science Engineering,
Maharishi University of Information Technology, Lucknow
[3]Faculty, School of Information and Communication Technology,
Gautam Buddha University, Gr. Noida.*

Abstract— Internet of Things (IoT) comprises smart devices, sensor nodes, and wearable elements for data sharing and services, through which the sensor networks are used for developing smart environments. IoT models are growing very fast because of the rapid growth of wireless devices and communications. In addition, the heterogeneous nature of the IoT paradigm heightens the risks to both individuals' data privacy and their data's security. As a direct consequence of this, comprehensive security models are required in order to guarantee secure communication between the various devices. The biggest obstacle in the way of effective and reliable device interaction in the Internet of Things is security.

Keywords- COAP mode control, GPS, Environment, Human Object, IOT.

I. INTRODUCTION

In the present scenario of human lives, Internet of Things (IoT) impacts in greater ways the various domains.

AUTHENTICATION IN IOT

Authentication in the IoT model is significant for developing trust in the identity of IoT elements and devices to secure the data and provide access control when the data travels through the insecure channel. Moreover, an efficient authentication model is required, which can provide trust over the linked IoT devices and elements and secure the data from unauthorized access. Authentication helps in preventing the devices from various attacks in the hope of secure data access from servers which includes conversations, images and some private data. Typically, strong authentication between nodes can be achieved in the following ways,

One-way Authentication

This is in the case where two entities are required to communicate with one another, in that, one entity should authenticate itself to another entity, and the other entity is not required to be authenticated.

Two-way Authentication

This can be otherwise called as mutual authentication, in which both parties are required to be authenticated with each other.

Three-way Authentication

In this case, a third party called central authority is required to authenticate the parties in the communication channel and make them authenticate with each other.

Distributed Authentication

In this method, a distributed straight authentication process is involved between the entities for secure communication.

Centralized Authentication

In this method of authentication, a centralized server called Trusted Third Party is used for distributing and managing the certificates for authentication.

II. KEY MANAGEMENT IN IOT

IoT key management process can be classified into three classes of protocols, as,

Centralized

In the centralized key management protocol, a single entity called Key Distribution Center (KDC) is used for accessing the group and provides the group encryption key for each entity.

De-centralized

The decentralized key management protocol is processed based on the key controller hierarchy for sharing the data and the encryption group key to all the entities for preventing the single-point failures.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6514
***Article Received**: 20 January 2023 **Revised**: 22 February 2023 **Accepted**: 02 March 2023*

Distributed

In the distributed key management protocol, the entities in the group are involved in deriving the common session-key.

The process of key management should be designed in such a manner to provide security, Quality of Service (QoS), and the key server resources. The cryptographic techniques are the basic in the process of key management in IoT. The IoT security model is to be designed to handle the heterogeneous network. The key management protocol must ensure the security requirements of IoT such as availability, data confidentiality, authentication, non-repudiation, and data integrity. Figure 4.4 displays the session key establishment in the process ensuring data integrity and confidentiality in IoT.

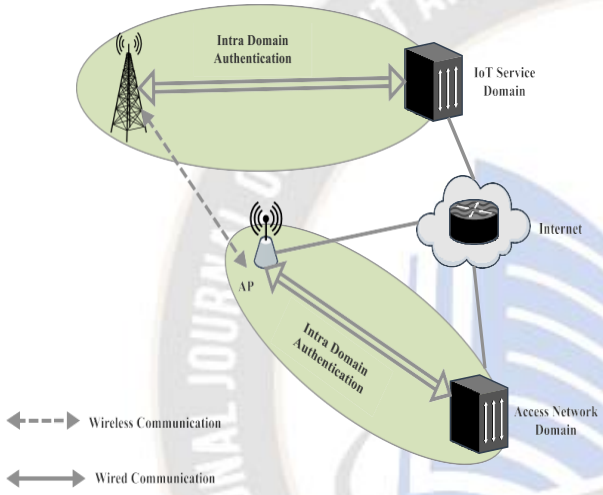

Figure 1 Process Of Authentication With Domain Networks

III. AUTHENTICATION MODULE

This section will offer you with information on the Physical Features based for Internet of Things networks. The tag is framed using the Trusted Third Party (TTP), and the public key is framed using the characteristics that were retrieved. The Overall Trust Value of an IoT element is determined by combining the results of two separate calculations: the Behavioral Trust Value and the Data Trust Value. The factors are determined by computing them based on the unique characteristics of the gadget. The resulting keys are used in the processing of the device authentication, which in turn takes into consideration the following factors:

- Key access that is determined by management requirements
- Determining the reasons behind the attackers' actions

Obtaining control over the process of encryption

It is essential that data be safeguarded at all times and transmitted using only trusted methods.

- An efficient method for handling the management of keys

Starting Suppositions and a Model of the System

In this scenario, an office setting is used to represent the Internet of Things (IoT) network architecture. A number of devices and a Trusted Third Party, sometimes referred to as TTP, are connected to one of the gateways. The following components make up the various aspects of the network model.

Authenticator The user's identity is verified via the authenticator throughout the digital authentication process. This verifies that the user is who they say they are.

TTP stands for "trusted third party," and it refers to an organisation that acts as a conduit for communication between two parties, both of whom place their faith in the third party. Due to the ease with which fake data may be generated, the independent third party investigates every significant transaction interactions that take place between the businesses.

Requester

The unit that has a need for a data, resource, or service to be processed is referred to as the requester.

Attacker

The unauthorised user, often known as the attackers, is the one who is attempting to get access to the data or to alter it.

The evaluation of the susceptible devices may be completed quickly and effectively thanks to the Trusted Third Party's familiarity with the common properties. The TTP is framed with the structure and determines the public key and secret key for each device when it is linked to the network. This happens when the devices are connected to the network. A device that accepts a message from another device, known as the requester device, is known as an authenticator. Figure 4.5 is a diagrammatic representation of the secure communication that may be achieved using TTP in the IoT.

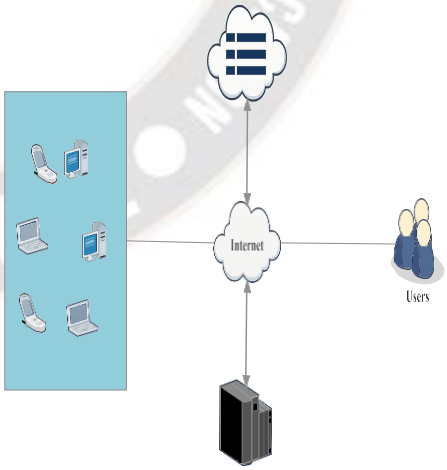

Figure 2 Secure IOT Communications With TTP

When the IoT devices are requested for communication, the Trusted Third Party (TTP) obtains the features of the devices for generating the public key and secret key for authentication. The steps for key generation are discussed in section Public Key.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6514
***Article Received**: 20 January 2023 **Revised**: 22 February 2023 **Accepted**: 02 March 2023*

Generation with General Features

In this case, public keys are generated taking into account common characteristics of Internet of Things devices. What's more, Authenticator is where you'll find the FRL, or Feature Revocation List. Table 4.1 lists the most often used qualities with Fitness Rate (FR) that are taken into account while generating keys.

Table 1 Features and Fitness Rate

Features	FR
type	1
asrc (bytes)	2
asest (bytes)	2
counta	1
eflag	1
Types	3
host_count	3
erv_count	2
erv_error_rate	4
rate	3
diff_serv_rate	3
serv_rate	2
diff_serv_rate	2
same_src_port	3
diff_src_port	3
serror_rate	5
attempts	5
creations	4
access_files	4
compromized	5

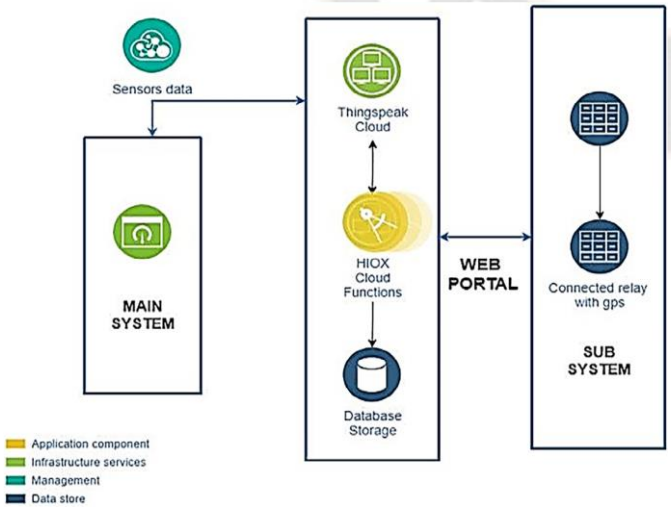

Fig 3 Cloud Architecture Overview

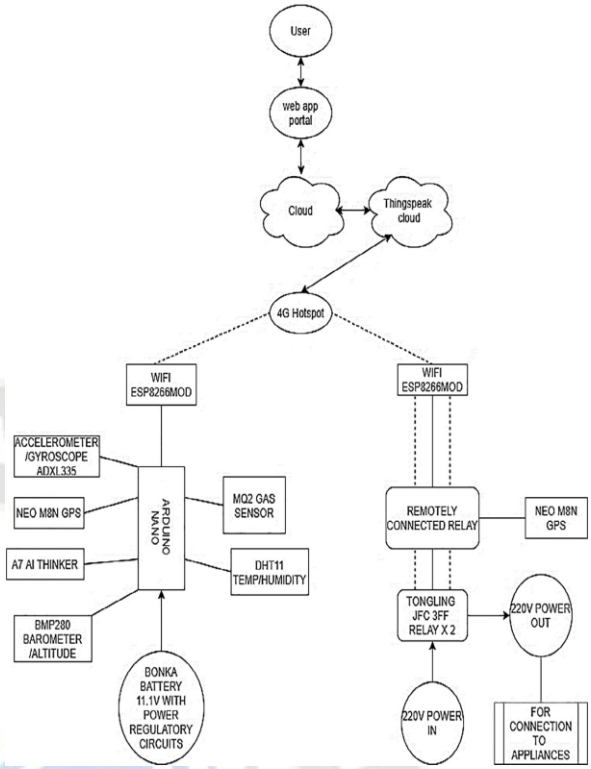

Fig 4 System Architecture

IV. RESULTS AND OBSERVATIONS

Session time is the network parameter defined as the specific time that is allowed to sustain a model in a specific operation. It can be determined as the period is terminated when the process takes place. This section describes the session time based evaluations and result comparisons, in which the session time is varying as 20, 40, 60, 80, and 100 seconds.

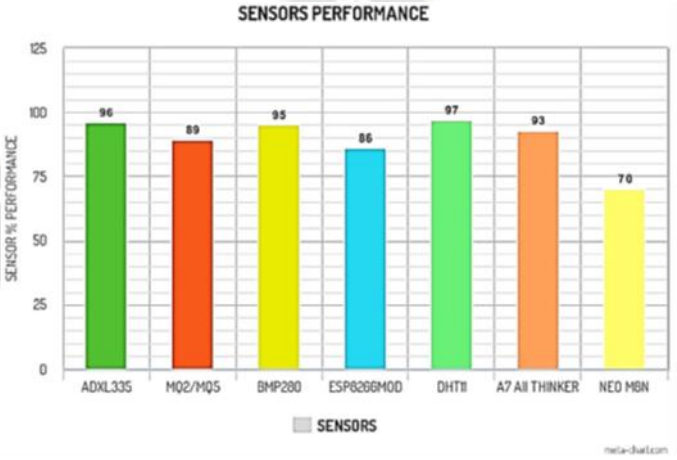

Fig 5 Percentage Performance Of Sensors Over Time.

V. CONCLUSION

From the graphs, it is depicted that the proposed model achieves 0.63% of high detection accuracy, 60% high resilience, 1% of high residual energy and 18% less computational cost than the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6514
Article Received: 20 January 2023 Revised: 22 February 2023 Accepted: 02 March 2023

compared model. It shows that the proposed model outperforms the compared one when it is analyzed with the factor, Session Time, which is evaluated in the rate as, 20, 40, 60, 80, and 100, in seconds.

From the graphs, it is depicted that the proposed model achieves 0.53% of high detection accuracy, 19.58% high resilience, 1% of high residual energy and 22.95% better computational cost than the SecureMatch model. It shows that the proposed model outperforms the compared one when it is analyzed with the factor, attack frequency, which is evaluated in the rate as, 50, 75, 100, 125 and 150, in kb/s.

To enhance the model effectiveness and the detection accuracy even higher, the next phase of work utilizes the Lion Optimization Algorithm (LOA). The work in the next phase is to detect anomalies that help to prevent malicious activity in the network.

References

[1] Abdul Rahman, Reem Shah, Babar. (2016). ‘‘Security analysis of IoT protocols: A focus in CoAP.” 1-7. 10.1109/ICBDSC.2016.7460363.

[2] D. Halabi, S. Hamdan, S. Almajali, ‘‘Enhance the security in smart home applications based on IOT-CoAP protocol,” digital-information,-networkingand-Wireless-communications.-(DINWC),-Beirut,-2018,-pp.81-85.doi: 10.1109/DINWC.2018.8357000.

[3] Hussain Fatima, Hussain Rasheed, Hassan Syed, Hossain Ekram. (2019). ‘‘Machine Learning in IoT Security: Current Solutions and Future Challenges”.

[4] J. Mišic´ , V.B. Mišic´ , Proxy cache maintenance using multicasting in CoAP IoT domains, IEEE Internet Things J. 5 (3) (2018) 1967–1976, https://doi.org/ 10.1109/JIOT.2018.2818115.

[5] Marco Lobe Kome, Frederic Cuppens, Nora Cuppens-Boulahia, Vincent Frey ‘‘CoAP Enhancement for a Better IoT Centric Protocol: CoAP 2.0” 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Vol. 00, 139-146, 2018.

[6] M.B. Tamboli, D. Dambawade, ‘‘Secure and efficient CoAP based authentication and access control for Internet of Things (IoT),” 2016 IEEE International Conference on Recent Trends-in-Electronics, Information-&-Communication Technology (RTEICT), Bangalore, 2016, pp. 1245-1250.

[7] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surveys Tutorials 21 (3) (2019) 2702–2733, https://doi.org/10.1109/COMST.2019.2910750.

[8] Victoria Beltran, Antonio F. Skarmeta , ‘‘An Overview on Delegated Authorization for CoAP Authentication and Authorization for Constrained Environments (ACE) ” in Editor (‘Book Security analysis of the constrained application protocol in the Internet of Things’ (IEEE, 2017, edn.), pp. 163-168.

[9] Wail Mardini, Muneer Bani Yassein, Mohammad Alrashdan, Abdalraheem Alsmadi, Ahmad Bani Amer ‘‘Application-based Power Saving Approach for IoT CoAP Protocol ” USA, 5 pages, 10.1145/ 3279996.3280008.