IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11710

# Designing Real-Time Systems with the Internet of Things: Strategies and Applications

**Deepak Tailor[1], Anand Bhaskar[2]**

M.Tech Student, Sir Padampat Singhania University, Udaipur, INDIA[1]

Professor Sir Padampat Singhania University, Udaipur, INDIA[2]

**Abstract:** The key to making any system intelligent is the internet of things. The requirements of the modern systems are met by using recent operating systems. Numerous platforms have been created for the Internet of Things. The majority of them, meanwhile, are designed for certain implementations and are unable to handle the present constraints of more modern systems. We will cover a broad overview of the Internet of Things, its working mechanism, resource constraints, node attributes, and mixed traffic communications in our research. We will also talk about newer technologies that make use of an Internet of things platform that has numerous uses. Current developments necessitate that modern gadgets be connected to the internet, which builds the modern Internet of things and improves user experience by ensuring a strong connection and efficient use of the devices belonging to the next generation. However, the increased connectedness of the Internet of Things has made it a target for attackers in recent times. We'll talk about common assaults, security risks, and modern Internet of things strategies.

**Keywords:** Internet of Things, Real-Time Systems

## I. INTRODUCTION

The quality of life is being improved by the internet of things, which is expanding quickly. The Internet of things is developing thanks in large part to enormous technological technologies and development. Hardware that is readily available and reasonably priced is essential for the system's constant evolution. The next step is to design Internet of Things operating systems to support the recently produced hardware in tandem with the existing methods and standards for all communication layers [1].

The availability of multiple Internet of things operating systems necessitates enabling interoperability, which calls for adherence to specific guidelines for development and functional capacity for supporting diverse deployment situations. The internet of things necessitates intelligence in order to adjust to network conditions. In that study, we'll give an overview of the many Internet of Things operating systems, improved hardware, and potential research areas. which will allow us to talk about the verified papers on our problem with the administration of Internet of Things operating systems: the opportunities, challenges, and potential solutions. We will eventually go over our findings and suggestions.

The main force underlying all of the technological transformation is the internet of things. The difficulty lies in the integration of unified technologies. Current advancements in "millimeter wave," contemporary cellular networks, the fifth generation of the smart Internet of things, wireless systems, device-to-device communication, Internet of things resources, and its operational systems, among other things. The next generation of the Internet of things is developed with the help of research. The development of Internet of Things technologies and their affordable availability have made devices more accessible and connected over long distances [1]. As a result, adhering to the standards is essential to enabling communication between the various Internet of Things networks. Manufacturing the Internet of things requires connecting industrial components in centralized or distributed ways to boost production and efficiency. The industrial revolution's fourth is still evolving. It poses significant difficulties for autonomous and intelligent systems, which must be clever enough to embrace machine learning methods in order to handle the massive volumes of information they generate.

### 1.1 OPERATIONAL MECHANISMS AND KEY CHARACTERISTICS: AN IN-DEPTH ANALYSIS

The Internet of Things device seeks to establish connections with other devices in order to share data. The Internet of Things platforms enable developers to create and implement Internet of Things by connecting sensors to networks. Numerous studies were conducted to support Internet of Things applications, taking into account the platforms and publications involved in comparing the various Internet of Things communication protocols, such as "Message Queue Transport," with other numerous protocols [2], 49. Using some files from sensor readings without the use of Internet of Things platforms, a comparison of four protocols was made, and the amount and parameters were looked into.

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

The researchers used many of these platforms for specific implementations, making use of the "message queue telemetry transport" protocol and incorporated ready-made hardware kits. For example, when the researchers implemented medical and healthcare technologies, they did not use previously developed Internet of things operating systems on their platforms. Using portable processors and an outdated operating system provides a broad platform [2].

Modern cyber and physical systems are closely intertwined with the Internet of Things. Current Internet of things systems can be identified as a broadly interconnected network with nodes that are connected and controllable remotely. Because of the additional existing limits, allowing security in modern Internet of things systems is typically more difficult than in general Internet of things systems. Our aim is to outline the characteristics, constraints, and security risks associated with the modern Internet of things, as well as to provide a summary of security solutions specifically tailored to address these vital safety concerns. While there have been some surveys conducted on privacy and security concerns in general Internet of things systems, there hasn't been a thorough conversation regarding security in recent years [3]. An overview of the Internet of things in recent times is displayed in Fig. 1. The wireless connection established by those devices is indicated by the blue lines. Every Internet of things device periodically completes specific activities required for

### 1.2 SAFETY REQUIREMENTS AND RESOURCE LIMITATIONS: BALANCING CONSTRAINTS IN SYSTEM DESIGN

Numerous modern Internet of things devices, such as sensors, controllers, autonomous cars, automated flying aircraft, etc., have extremely limited resources, such as processors, memory, batteries, etc., and typically require electricity to complete operations that take several milliseconds. Modern Internet of things nodes also require the fulfillment of time-based attributes. Deadlines are typically used to describe certain attributes [5].The significance of the outcomes produced the system lowers when a deadline is missed. If the value quickly declines, we regard the system as a recent firm system, similar to "antilock braking" systems in cars and nuclear power plants.

### 1.3 CHARACTERISTICS OF MODERN INTERNET OF THINGS NODES: A CONTEMPORARY OVERVIEW

When used as a schedule of recurring chores, stringent time constraints and deadlines, The worst situations and limits are well-known, No loaded or dynamically self-adjusting codes, Recursion is severely statically constrained or not utilized at all. Processing and memory power are typically limited [6].

### 1.4 MANAGING MIXED TRAFFIC IN COMMUNICATION NETWORKS: CHALLENGES AND SOLUTIONS

Numerous conventional modern time systems are made up of different nodes that function separately and have either little or no connectivity capabilities. However, as the Internet of Things has evolved, physical and cyber nodes now communicate with each other through industrial networks and are typically connected via the Internet. Supporting these applications requires a current time channel for communication with a certain service quality, as well as the amounts and requirements for processing data, among other things, because the majority of recent apps require triggering events based on specific information conditions [7].

Additionally, the modern Internet of things has the characteristic of typically incorporating traffic flows with varying degrees of relevance, such as those with varying degrees of bandwidth, availability, and timeliness needs. High priority traffic, such as sensors for closed circuit control and actual control orders in avionics, automotive systems, and home security systems, is essential for the safe and proper operation of the system.
The medium priority traffic, which is essential for the proper operation of the system but has some delays, drops, etc.; for instance, aircraft navigation systems, power substation system monitoring, communication messages between electric vehicles and charging stations, heating, water sprayers in stations, air conditioning, lighting devices, food preparation machines, etc [8].

The lowest priority traffic, which consists primarily of all other system traffic that doesn't need bandwidth guarantees or delays, includes notifications and messages from smart home machines, multimedia flows in aircraft, and engineering traffic in power substations.

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

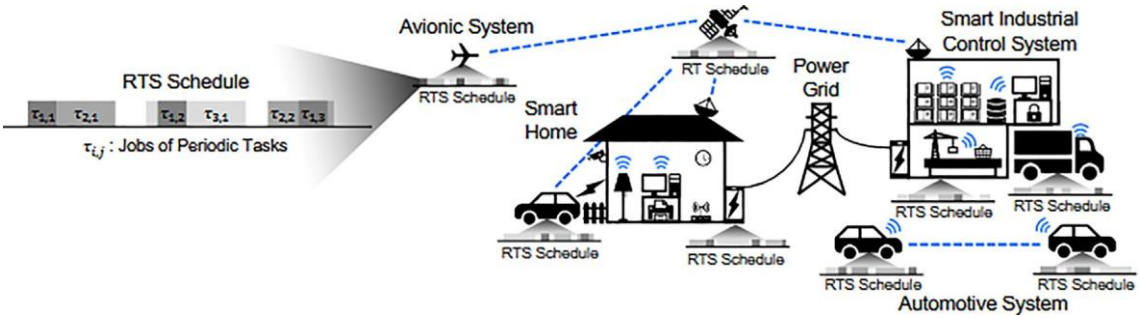


Fig. 1. Overview of daily recent time Internet of things.

**2.** The features of all the high criticality flows are typically well known in many critical recent Internet of things of safety, whereas the properties and quantity of the other flows are often dynamic [10].

### 1.5 LATEST TECHNOLOGIES

It may appear like nothing new to have contemporary resources close to established data resources. In order to increase efficiency and performance, a system that allows program techniques and the relevant information to be distributed to the edge of a network was initially described as "edge computing" in 2004. Furthermore, in 2009, the concept of utilizing virtualization technology based on computer resources within the Wi-Fi subsystem was developed. However, it wasn't until "fog computing" for the Internet of Things was introduced that there was a genuine interest in increasing resources for computing at the network's edge. Researchers have been using a variety of words in recent years to illustrate similar approaches with "fog computing." For example, the concept of cloud computing at the network edge was described by the author of cloudlet, which is built on virtual machines, using the term "edge computing." Furthermore, the author's most recent work demonstrated that fog is a component of "edge computing" [11].

It is obvious that the primary goal of cloudlets was to replace mobile apps from distant clouds with closer cloudlet virtual computers located in similar Wi-Fi subsystems, for the purpose of distributing computationally demanding activities. The goal of the original "fog computing" presentation, however, was to spread the cloud to the network's gateways in order to complete it. In this regard, cloudlet might be regarded as one of the useful techniques for "fog computing" in the presence of nearby server equipment. Fog computing, also known as "Edge Computing of Multiple Accesses," is described in numerous other works. Essentially, "Edge Computing of Multiple Accesses" was introduced by the European Institute of Standards and Telecommunications as a specific standard from the perspective of telecommunications. In this standard, the European Institute of Standards and Telecommunications specified the Interface of Programming standards about how telecom companies are able to provide computing services based on virtualization to their clients based on expanding the infrastructure that is already in place for virtualization of network functions, "Edge and Fog Computing," and the Internet of things [11].

However, according to the current collaboration between "Open fog" and The European Institute of Standards and Telecommunications, "Edge Computing of Multiple Accesses" is not the same as "fog." The realization of "fog computing" will be accelerated by the application of "Edge Computing of Multiple Accesses." In older phases, "fog" was also referred to as "mist computing." However, mist was previously referred to as a subset of "fog" in current literature. Consequently, we concentrated on the necessity of distributing computing mechanisms to the Internet of Things extreme edge, where the devices are located, in order to reduce the latency of communication between Internet of Things devices to milliseconds [12]. The goal of "mist computing" is essentially to enable self-recognition in terms of self-organization, self-management, and diverse self-methods for Internet of Things devices. As a result, Internet of Things devices will be able to continue working even in the event of an unreliable internet connection. In general, "mist" devices may sound similar to fixed services or mobile web services, where applications are incorporated into a variety of devices with limited resources, such as actuators, cell phones, and sensors.

However, "mist" refers to the capacity for self-awareness and situational recognition, which enables the remote deployment of dynamic software code to various devices based on changes in the environment and the state of the devices themselves. Similar to "fog" in providing a framework that enables adaptable software deployment and reconfigurations [12]. In light of this, it follows that "fog" requires the support of all linked "edge computing" technologies. In other words, no one can install or manage "fog" without integrating "edge computing" technologies.

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

## 1.6 CONTEMPORARY SECURITY THREATS AND ATTACKS IN THE INTERNET OF THINGS

Various threats can affect modern Internet of things systems in different ways, depending on the objectives and architecture of the adversary. One of the contributing vendors may act maliciously in a system built using a vendor-based paradigm. That potentially unreliable vendor has the ability to infiltrate the system and carry out a number of malicious operations. Also, even in cases where the contributing vendors are not hostile, poor coding techniques may result in vulnerabilities. The adversary may target the communication interfaces in a system with a network connection. Since most of such systems lacked authentication, it was simple to counterfeit and intercept communication channels.

Attack techniques against the Recent Time Strategy are classified based on the attacker's functional goal and control over the computing processes. The installation of a malicious virus or code, or the use of the law for evil purposes, is the only means of taking control of a target machine. Furthermore, the system is vulnerable to network assaults because nodes in the modern Internet of things can communicate over untrusted channels like the internet [14]. Apart from the constant attempts to forcefully crash the system. By silently attaching to the system, the adversary may be able to get sensitive data through attacks on select channels. Attacks against the subset channels rely on identifying system characteristics such memory usage patterns, task scheduling, power consumption, etc. The attackers may utilize such information in the future to conduct more assaults.

## 1.7 RECENT CYBER ATTACKS ON INTERNET OF THINGS SYSTEMS

- Integrity breach due to introduction of harmful codes: A cunning adversary may get access to the system. In order to avoid quick detection and harm one or more of the current recent jobs, an adversary could, for example, add a spiteful task that complies with the system's recent promises. The attacker could use that task to manipulate sensors and change the system's behavior in ways that are not desired [14], 101.

- Integrity breach brought about by the introduction of malicious codes: The system may be accessed by a crafty adversary. An enemy might, for instance, introduce a nasty work that complies with the system's recent promises in order to evade rapid discovery and damage one or more of the existing recent jobs. With that task, the attacker might modify sensors and alter the system's behavior to their liking [14].

A subset channel assault modifies previously unidentified channels in order to obtain important information from the victim. Some of the subset channels that the attackers employ are memory access, power usage traces, scheduling preemptions, temperature, etc. Because of the deterministic activities in these systems, those attacks are especially suitable to assaulting nodes of the Recent Time Internet of Things that implement Recent Time tasks [14].

- Attacks on communication channels: In the modern day, the Internet of Things has elevated the internet as the primary means of communication between entities. However, the internet poses a number of vulnerabilities that could jeopardize the security and privacy of modern Internet of things devices, making it an unsafe medium of communication.

- Interception or spying, falsification, interference with control, and informational messages are among the threats to communication. From the perspective of the modern Internet of things, communication hazards are difficult to defend against. This is due to the difficulty in distinguishing between legitimate and rogue communication traffic, especially when it comes to high-priority communication, without compromising service quality [15].

- "Cryptographic" protection measures are frequently included to tackle communication threats. However, this raises the bar for wireless task communication engineering technologies and may require current scheduling adjustments. Numerous cryptographic processes are extremely costly to execute on constrained resources, particularly those found in fixed devices of the modern Internet of things. Thus, current cryptographic techniques may not be the preferred choice for many modern Internet of things systems. There is a way to integrate security mechanisms that can be used to address communication threats without requiring changes to the recent efforts that are now underway [15].

- Attacks of service denial: Nodes of the recent Internet of things are vulnerable to attacks of service denial because to resource limits such as low memory capacities, restricted processing resources, etc., and stringent time constraints.An attacker might take over open tasks and deplete system resources like memory, the disk, and the CPU. The attack of distributed services denial, in which numerous malicious nodes target the devices concurrently, is a more dangerous kind of service denial attack. An attacker may hijack network ports and launch an attack on the network to compromise system integrity and privacy, especially when important tasks are scheduled to begin [16].

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

The defense mechanisms designed for general information technology or fixed systems are not easily adaptable without significant changes, and they do not take into account the timing, resource limitations, or safety of the modern Internet of things. Our recent efforts could be combined to defend against denial-of-service assaults. However, the attacker must first conduct research and attack preparation in order for these attacks to be successful. That will be covered in the following:

## II. MODERN APPROACHES TO PROTECTING INTERNET OF THINGS SYSTEMS FROM CYBER ATTACKS

These methods could be divided into two major categories:
1. Products that require specific hardware support in order to offer security.
2. Software-level solutions that don't require modifications.
First, hardware-supported protection:

The "Simplex" structure is key to providing protection without compromising system security. The well-known "Simplex" time structure was developed recently and relies on a modest safety controller to take over in situations where a complex high-performance controller is either absent or malfunctioning [16]. The aim of the "Simplex" method is to ensure that a system remains safe even if it is controlled by an intricate controller. The basic idea behind the "Simplex" structure for protection is to use a slightly streamlined system to keep an eye on the characteristics of an unreliable entity that is assigned to more difficult responsibilities, such as its behavior over time, memory access, system call traces, abnormalities, etc. Second, protection without any changes: Although architectural changes can strengthen the security posture of nodes in the recent Internet of Things, these methods require a general redesign and may not be appropriate for systems that have been developed that use connection-oriented transport components of service [16].

### a. RECENT SOFTWARE-BASED APPROACHES FOR ENHANCING PROTECTION IN INTERNET OF THINGS SYSTEMS: AN OVERVIEW

Handling subset channel attacks: It has been shown that the attacker is able to execute a timed attack to indirectly estimate memory use behavior. The majority of recent Internet of things systems that rely on connection-oriented transport services lack isolation for dispersed resources among various workloads. When the system switches between different tasks, there is overlap between the tasks. Therefore, in order to prevent assaults on subset channels, it becomes important to capture the protection constraints between the tasks.

Integrating safety into the Internet of Things in real time has been suggested by the introduction of methods for imposing constraints on the tasks that have recently been scheduled with a high priority. The scheduler clears the distributed cache when the system switches from a work with high protection, which requires greater privacy, to a task with low protection, which is an unprotected task that is primarily damaged, based on the defined degrees of protection for each task [18].

## III. INTERNET OF THINGS PLATFORMS: STRATEGIES AND BEST PRACTICES

Utilizing the Internet of Things platform, which offers the essential features of modern operating systems, we developed a few apps. The hardware stratum includes actuators, sensors, and communication modules. The following forthcoming sub-systems are necessary for the construction of the Internet of things system:

- The Internet of Things prototyping platform, which enables the development of Internet of Things nodes; the Internet of Things server, which facilitates communication between nodes; the structure that describes the data exchange process; and the communication protocol, which regulates the message transfer between the Internet of Things nodes and the recent time server.

The recommended system provides connectivity and dependability to a wide range of intelligent Internet of things applications, enabling optimal use of it. The ARM Cortex-M40 is used to implement the recommended Internet of Things platform. Due to its appropriate and robust power consumption, a smart phone can serve as the recommended Internet of Things node. The core components of the proposed system are the Internet of Things key server and nodes. Using the internet as a reliable backbone, the key server manages communication between the system's nodes, Figure 2 [18].

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

**a. CLASSIFICATION OF SYSTEM NODES: A CATEGORICAL OVERVIEW OF FOUR MAJOR TYPES**

- "Sensor" nodes that are aware of their environment.
- "Actuator" nodes that affect their environment.
- "Hybrid" nodes that are aware of and react to their environment.

### 3.2 COMPREHENSIVE DISCUSSION OF THE SYSTEM: IN-DEPTH EXPLORATION AHEAD

Internet of Things nodes : The proposed platform is a fixed system that can be designed for any type of controller that satisfies the system requirements. It was developed, implemented, and successfully operated in the experiments.

The ARM Cortex-M40 processor, which powers the suggested model, is specifically made for high performance, low power consumption, and affordable devices, making it ideal for Internet of Things nodes. The suggested model is implemented using the "Nucleo Board." Each node is made up of a controller, which is needed to manage the operations of the node, WI-FI hardware, which is used to connect wirelessly to the network and access the internet, and sensors, which are used to sense the environment [19].

The system's nodes are divided into four main categories based on how they are connected to the key server to carry out certain functions: sensor, actuator, hybrid, and monitoring nodes.

The "Sensor" nodes are nodes that include one or more sensors but no actuators. They are used to perceive their environment and periodically send the information they sense to the server within a predetermined amount of time. The "Actuator" nodes, which comprise one or more actuators and lack any sensors, influence the environment in response to commands from the monitoring nodes [19].

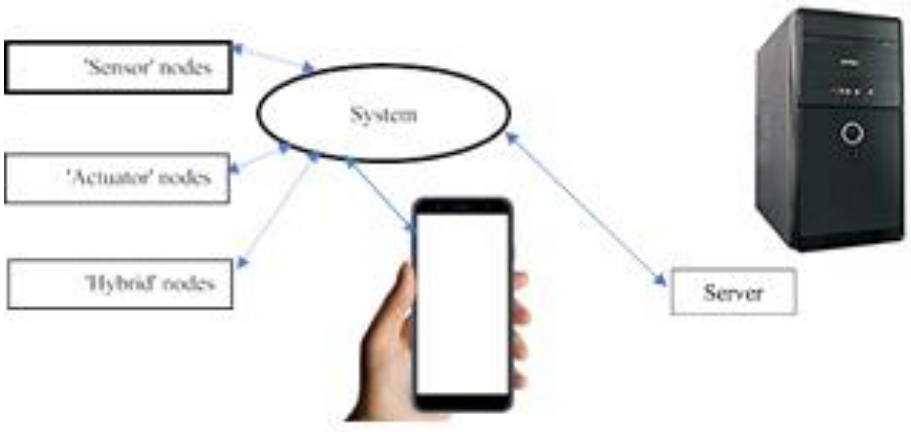


Fig. 2. The suggested structure of system of Internet of things.

The actuator and sensor nodes are combined into the "Hybrid" nodes. These are nodes that have both actuators and sensors. The node's operation involves initially establishing communication with the Internet of Things server, sending sensor data to the server, and receiving commands from the monitoring nodes throughout the server to carry out. Smartphones that manage and keep an eye on the system nodes could be the monitor nodes. These are the nodes that lack sensors and actuators, but they manage the actuators and keep an eye on the readings from the sensors by transmitting orders and obtaining and processing sensor data.

### 3.3 THE ROLE AND FUNCTIONALITY OF IOT SERVERS

The Internet of Things Server is the essential system component that enables communication between all of the system's nodes. It can communicate with any kind of node and enables nodes to monitor and visualize sensor data [19]. The server will send its data to the registered monitors if the connected node is a "Sensor" node. Additionally, the server will forward the commands from the monitoring nodes to the node if it is a "Actuator" node. Additionally, in the event that the node is a "Hybrid," the server will handle tasks for both the actuator and sensor nodes jointly; in the event that the node is a "Monitoring" node, the server receives orders, forwards them to the actuator nodes, and forwards sensor data to this "Monitoring" node [21] Fig. 3.

  

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11710

### 3.4 PROPOSED COMMUNICATION PROTOCOLS FOR ENHANCED IOT CONNECTIVITY

The key server is in charge of facilitating communication between the system's nodes so that tasks can be completed. Each node opens a connection of protocol for control of transmission with the key server and authenticates itself to the system by sending its identification number to the key server while awaiting the server's acknowledgement.

The "Hybrid" node performs the duties of both the actuator and the sensor nodes. The "Sensor" node identifies itself and is then prepared to transmit the periodic information that it possesses. The "Actuator" node receives orders from the "Monitoring" nodes across the key server following the identification process. Following identification, the "Monitoring" node registers to collect data from particular sensor nodes and sends commands to particular actuator nodes [21], 13. Nodes communicate with each other through the server. Each node attempts to identify itself and establish a connection; if the server acknowledges it, the nodes can effectively communicate with one another.

### 3.5 EXPERIMENTAL SETUP: METHODOLOGY AND CONFIGURATION

adjusting different network factors that affect the protocol performance, experiments are conducted to examine the performance of the proposed communication protocol and the "Message Queuing Telemetry Transport" protocol [22].The total transferred bytes for each message that is successfully transmitted and the length of delay—which is the difference between when the message is published and when the server acknowledges it—are the performance metrics that are evaluated. Three machines are utilized in the setup: a laptop that runs a wide-area network emulator software to simulate channel losses and communication delays, a personal computer that serves as a server to facilitate communication between the platforms, and another laptop that functions as a node for publishing messages and awaiting acknowledgement. The total transferred bytes for each message that is successfully transmitted and the length of delay—which is the difference between when the message is published and when the server acknowledges it—are the performance metrics that are evaluated.

Three machines are utilized in the setup: a laptop that runs a wide-area network emulator software to simulate channel losses and communication delays, a personal computer that serves as a server to facilitate communication between the platforms, and another laptop that functions as a node for publishing messages and awaiting acknowledgement.

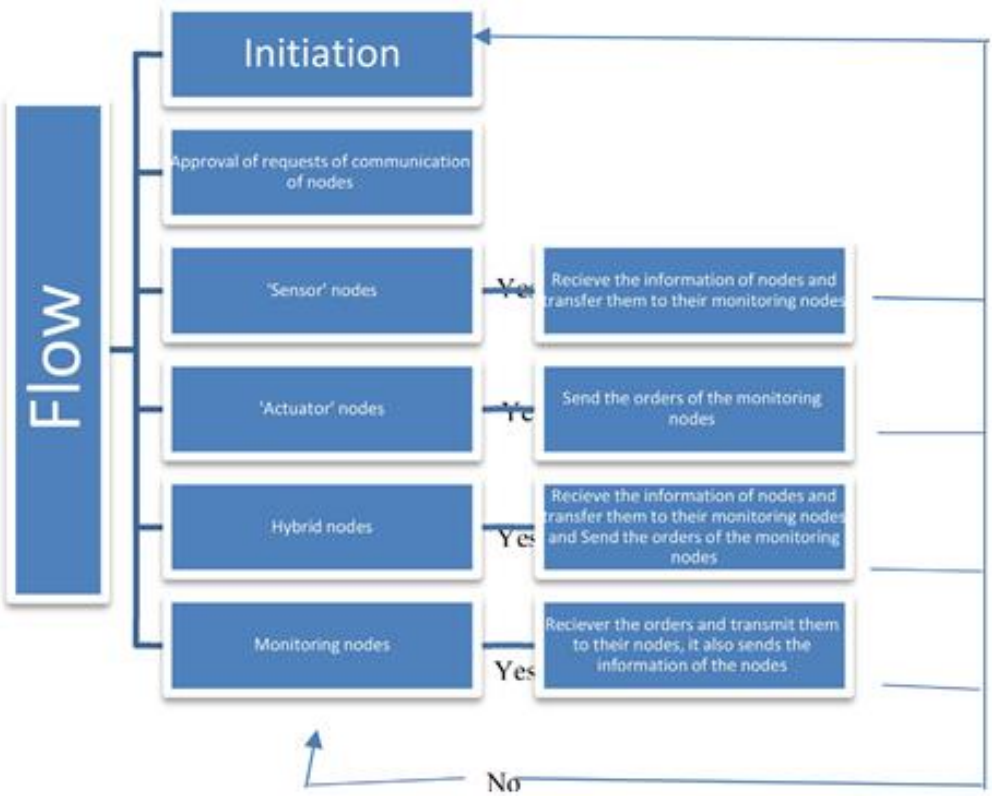


Fig. 3. The flow of data across the server of Internet of things.

  

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11710

### 3.6 RESULTS OF THE EXPERIMENT

The two protocols were able to deliver their messages without worrying about the percentage of loss applied in the one node and one server experiment setup. This indicates that the two protocols have a good message delivery technique for working with the various rates of losses, and the performance assessments are examined for message delays and the total amount of data transmitted for each successfully transmitted message. The metric of message delay is important, particularly for recent systems where time is even more important. The protocol of "Message Queuing Telemetry Transport," or "MQTT," with a certain level of service quality is compared with the recommended protocol of communication with a certain level of acknowledgment for similar messages [22], 87. The applied rates of losses affect the message delay because retransmissions are necessary to deliver the message successfully.

## IV. CONCLUSION

The term "Internet of things" refers to the recent trend of smart devices such as smart televisions, home automation systems, and webcams being connected to the internet. This connects previously isolated items and applications. The intricacy of contemporary cyberattacks on the Internet of Things necessitates reconsidering methods for safeguarding these systems. The purpose of this work is to bridge the gaps between the current security of Internet of Things systems and the latest limits, as well as to increase knowledge of recent time protection. The methods presented here range from hardware-assisted protection to protection that requires no modifications. The research produced a recommended Internet of Things system.

## REFERENCES

[1]. F. Al Turjman, Artificial Intelligence in IoT, Springer Science & Business Media, Berlin, Germany, 2019, pp. 93–105.
[2]. Cassimally, H. & McEwen, A., Designing the Internet of Things, John Wiley & Sons, United States, 47-54.
[3]. Brooks, T., (2017), Cyber-Assurance for the Internet of Things, John Wiley & Sons, United States, 129-132. (2013).
[4]. B. Alhayani, H. Ilhan, Efficient cooperative imge transmission in one-way mult- hop sensor network, Int. J. Electr. Eng. Educ. 57 (2) (2020) 321–339.
[5]. L. Zhang, D. Georgakopoulos, Internet of Things – ICIOT 2018, Springer Science & Business Media, Berlin, Germany, 2018, pp. 70–74.
[6]. P. Waher, Mastering Internet of Things, Packt Publishing, United States, 2018, pp. 308–314.
[7]. P. Friess, O. Vermesan, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, Netherlands, 2013, pp. 48–51.
[8]. M. Qiu, Smart Computing and Communication, Springer Science & Business Media, Berlin, Germany, 2018, pp. 103–108.
[9]. M. Agueh, R. Zitouni, Emerging Technologies for Developing Countries, Springer Science & Business Media, Berlin, Germany, 2018, pp. 32–40.
[10]. Hassan, Q., Internet of Things A to Z: Technologies and Applications, John Wiley & Sons, United States, 113-124. (2018).
[11]. Buyya, R. & Srirama, S., Fog and Edge Computing: Principles and Paradigms, John Wiley & Sons, United States, 103-112. (2019).
[12]. B. Alhayani, A.A. Abdallah, Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN, Eng. Comput. 37 (9) (2020) 1–17.
[13]. Li, S. & Xu, L., Securing the Internet of Things, Syngress, United States, 97-108. (2017).
[14]. Hu, F, Security and Privacy in Internet of Things (IoTs), CRC Press, United States, 355-368. (2016).
[15]. Gilchrist, A., IoT Security Issues, Walter de Gruyter, Berlin, Germany, 130-142. (2017).
[16]. B. Alhayani and Milind Rane,"face recognition system by image processing" International journal of electronics and communication engineering & technology (IJCIET),vol.5, no.5, pp. 80–90. 2014.
[17]. Cheruvu, S. & Kumar, A. & Smith, N. & Wheeler, D., Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment, Apress, United States, 5-40. (2019).
[18]. Kantarci, B. & Oktug, S., Wireless Sensor and Actuator Networks for Smart Cities, MDPI, Switzerland, 56-74. (2019).
[19]. Bilal Al Hayani, Haci Ilhan, Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring, J. Med. Imag. Health Inform. 10 (1) (2020) 160–168.
[20]. J. Park, H. Shen, Y. Sung, H. Tian, Parallel and Distributed Computing, Applications and Technologies, Springer Science & Business Media, Berlin Germany, 2019, pp. 130–142.

  

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11710

[21]. Cristian, G. & García-Díaz, V. & García-Bustelo, B. & Lovelle, J., Protocols and Applications for the Industrial Internet of Things, IGI Global, United States, 85- 93. (2018).

[22]. Sujit Kumar et al 2021. Strategies to Enhance Solar Energy Utility in Agricultural Area of Rajasthan State, India. J. Phys.: Conf. Ser. 1854 012013. DOI 10.1088/1742-6596/1854/1/012013

[23]. Sujit Kumar et al 2021. Dynamic Wireless Power Transfer in Electric Vehicles. J. Phys.: Conf. Ser. 1854 012014, 10.1088/1742-6596/1854/1/012014.

[24]. Vyas, S., Joshi, R.R., Kumar, V. (2022). An Intelligent Technique to Mitigate the Transient Effect on Circuit Breaker Due to the Occurrence of Various Types of Faults. In: Bansal, R.C., Zemmari, A., Sharma, K.G., Gajrani, J. (eds) Proceedings of International Conference on Computational Intelligence and Emerging Power System. Algorithms for Intelligent Systems. Springer, Singapore.

[25]. Vyas, M., Kumar, V., Vyas, S., Swami, R.K. (2023). Grid-Connected DFIG-Based Wind Energy Conversion System with ANFIS Neuro-Fuzzy Controller. In: Namrata, K., Priyadarshi, N., Bansal, R.C., Kumar, J. (eds) Smart Energy and Advancement in Power Technologies. Lecture Notes in Electrical Engineering, vol 927. Springer, Singapore.

[26]. Vyas, M., Yadav, V.K., Vyas, S., Swami, R.K. (2022). An Intelligent Control Strategy for Power Quality Improvement of DFIG-Based Wind Energy Conversion System. In: Kumar, J., Tripathy, M., Jena, P. (eds) Control Applications in Modern Power Systems. Lecture Notes in Electrical Engineering, vol 870. Springer, Singapore.

[27]. Vyas, M., Yadav, V.K., Vyas, S., Joshi, R.R. and Tirole, R. (2022). A Review of Algorithms for Control and Optimization for Energy Management of Hybrid Renewable Energy Systems. In Intelligent Renewable Energy Systems (eds N. Priyadarshi, A.K. Bhoi, S. Padmanaban, S. Balamurugan and J.B. Holm-Nielsen).

[28]. Sasanka Sekhor Sharma, RR Joshi, Raunak Jangid, Shripati Vyas, Bheru Das Vairagi, Megha Vyas., 2020, MITIGATION OF TRANSIENT OVER-VOLTAGES AND VFTO EFFECTS ON GAS INSULATED SUBSTATION. Solid State Technology, Volume 63, Issue 5/

[29]. S. V. . . et. al., “Life Extension Of Transformer Mineral Oil Using AI-Based Strategy For Reduction Of Oxidative Products”, TURCOMAT, vol. 12, no. 11, pp. 264–271, May 2021.

[30]. Y. Joshi, J. K. Maherchandani, V. K. Yadav, R. Jangid, S. Vyas and S. S. Sharma, "Performance Improvement of Standalone Battery Integrated Hybrid System," 2021 7th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 2021, pp. 250-255, doi: 10.1109/ICEES51510.2021.9383636.

[31]. Tirole, R., Joshi, R.R., Yadav, V.K., Maherchandani, J.K. and Vyas, S. (2022). Intelligent Control Technique for Reduction of Converter Generated EMI in DG Environment. In Intelligent Renewable Energy Systems (eds N. Priyadarshi, A.K. Bhoi, S. Padmanaban, S. Balamurugan and J.B. Holm-Nielsen).

[32]. Chhipa, Abrar Ahmed and Vyas, Shripati and Kumar, Vinod and Joshi, R.R., MPPT optimisation techniques and power electronics for renewable energy systems: wind and solar energy systems. International Journal of Swarm Intelligence, volume 7, number 2, pages 141-167, year 2022, doi : 10.1504/IJSI.2022.123092,:

  