JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DATA CENTRIC MACHINE-TO-MACHINE COMMUNICATION.

[1]Ujwal C, [2] Raju P, [3]Shreyas B T, [4]Venu Reddy K S,

[5]Mrs. Dhivya V

[1,2,3,4] B.E Student, Department of CSE, Sir M Visvesvaraya Institute of Technology, VTU, Bengaluru, India
[5]Assistant Professor, Department of CSE, Sir M Visvesvaraya Institute of Technology, VTU, Bengaluru, India

Abstract: In today's interconnected era, the integration of Raspberry Pi and robust security algorithms alongside the burgeoning Internet of Things (IoT) landscape serves as a pivotal force in fortifying privatized network devices against potential intrusions. This amalgamation capitalizes on connectivity as the backbone, facilitating seamless communication and information exchange among myriad devices. With the exponential growth of the Internet, the opportunity to establish private networks has blossomed, emphasizing not only connectivity but also safety. Leveraging emerging IoT technologies, including electronic hardware and protocols, offers new avenues for device interconnection and communication while ensuring stringent security measures are in place. This comprehensive literature review delves into diverse methods, protocols, and middleware platforms enabling the creation of privatized networks for various applications. Highlighting prevalent protocols such as MQTT, VSL, CoAP, AMQP, and the Data Distribution Service (DDS), it emphasizes the significance of real-time, scalable data distribution in distributed systems. Central to the discussion is the integration of Raspberry Pi's versatility and affordability, to ensure the resilience of privatized network devices and enhance the overall integrity and security of IoT ecosystems.

Index Terms **- Raspberry Pi, ESP8266, MQTT (Message Queuing Telemetry Transport), DDS (Data Distribution Service), UDP (User Datagram Protocol).**

I. INTRODUCTION:

In the modern era of interconnectedness, the integration of advanced technologies like Raspberry Pi and robust security algorithms within the expanding Internet of Things (IoT) landscape plays a pivotal role in fortifying network devices against potential intrusions. This integration harnesses the inherent connectivity of our digital ecosystem, facilitating seamless communication and information exchange among a plethora of interconnected devices. As the Internet continues to experience exponential growth, the opportunity to establish private networks has become increasingly accessible, emphasizing not only the importance of connectivity but also, the paramount significance of safety and security.

The utilization of emerging IoT technologies, encompassing electronic hardware and cutting-edge protocols, opens up new avenues for device interconnection and communication while ensuring stringent security measures are in place to safeguard against potential threats. This comprehensive literature review embarks on a journey through diverse methodologies, protocols, and middleware platforms, elucidating their pivotal roles in enabling the creation of privatized networks tailored to various applications.

A particular emphasis is placed on the exploration of prevalent protocols such as UDP, MQTT, VSL, CoAP, AMQP, and the Data Distribution Service (DDS), which serve as the backbone for real-time, scalable data distribution in distributed systems. Furthermore, the integration of Raspberry Pi, renowned for its versatility and affordability, is highlighted as a cornerstone in many IoT deployments, offering a robust platform for device interconnection and data processing.

As technology continues to advance at a rapid pace, the integration of Raspberry Pi and robust security algorithms represents a significant step towards enhancing the resilience of privatized network devices and safeguarding against potential threats. By delving into diverse methods, protocols, and middleware platforms, this literature review aims to provide valuable insights into the intricate landscape of IoT security, empowering readers to make informed decisions regarding their project's messaging protocols and electronic platforms.

II. RESEARCH OBJECTIVE:

The primary objective of this study aims to investigate the role of integrating Raspberry Pi and robust security algorithms in fortifying network devices within the expanding Internet of Things (IoT) landscape. The primary objective is to explore the utilization of emerging IoT technologies, methodologies, protocols, and middleware platforms to enable the creation of privatized

networks tailored to various applications while ensuring stringent security measures are in place to safeguard against potential threats. Specifically, the research will focus on examining prevalent protocols such as UDP, MQTT, VSL, CoAP, AMQP, and the Data Distribution Service (DDS) as backbone technologies for real-time, scalable data distribution in distributed systems. Furthermore, the study will assess the integration of Raspberry Pi as a cornerstone in many IoT deployments, offering a robust platform for device interconnection and data processing. By delving into diverse methods, protocols, and middleware platforms, this research aims to provide valuable insights into the intricate landscape of IoT security, empowering stakeholders to make informed decisions regarding messaging protocols and electronic platforms for their IoT projects.

III. LITERATURE REVIEW:

In 2023, Arya Yudidharmaa, Nicholas Nathaniela, Tang Nyquel Gimlia, Said Achmada, Aditya Kurniawan [1] proposed "A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes". This paper conducts a systematic literature review to identify prevalent messaging protocols and electronic platforms utilized in IoT-based smart homes. MQTT emerges as the favored protocol due to its efficient packet transfer and wide network bandwidth. CoAP exhibits resilience against network failures, while AMQP handles larger messages but impacts data transmission volume. DDS, despite lacking scalability, offers broker-less communication. Raspberry Pi, Arduino, and ESP8266 are commonly employed electronic platforms. Future research should assess protocol performance across varied platforms to determine effectiveness.

In 2023, Marco Esposito, Alberto Belli, Lorenzo Palma and Paola Pierleoni. [2] proposed "Design and Implementation of a Framework for Smart Home Automation Based on Cellular IoT, MQTT, and Serverless Functions". It proposes a flexible framework for smart home automation using MQTT and serverless computing. The framework incorporates vocal command interfaces for enhanced accessibility. A smart kitchen fan, equipped with an NB-IoT module, demonstrates the framework's viability. Evaluation shows NB-IoT's acceptable latency for MQTT messaging, with occasional packet loss. The framework utilizes Amazon Lambda and ASK for cloud deployment, enabling quasi-real-time interactions between users and smart objects. This approach offers potential for additional services like predictive maintenance, leveraging cellular connectivity and cloud resources.

In 2023, Vasilios A. Orfanos, Stavros D. Kaminaris, Panagiotis Papageorgas , Dimitrios Piromalis and Dionisis Kandris. [3] proposed "A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications". This review compares IoT-based networking technologies for home automation, highlighting affordability, performance, and coverage as key considerations. It aims to aid end-users, installers, and administrators in selecting the most suitable technology based on specific metrics. The comprehensive survey encompasses factors like adoption rates, technical characteristics, and collision avoidance. It underscores the need for a common interface to facilitate communication among diverse technologies, emphasizing the importance of focusing on shared characteristics such as medium, OSI layers, and data exchange protocols for effective integration.

In 2023, Abeye Tewodros, Ananya Samuel, Ebenezer Mulugeta, Nawid Barakzai, Sal Sabila Kouser, Dr. Vijay Kumar. [4] proposed work "Wireless Communication Without Internet Connection". It addresses the challenge of communication in areas lacking internet access by proposing a versatile messaging application utilizing WiFi-Direct. Unlike existing solutions with limited functionalities, the developed app offers comprehensive features including messaging, file sharing, screen sharing, and audio/video conversations. Leveraging WiFi-Direct, known for its high throughput and low delay, the app provides a practical solution for wireless communication in internet-restricted environments.

In 2019, Georg Aures, Christian Lübben [5] This survey conducts a comparative analysis of three IoT middleware technologies—DDS, MQTT, and VSL—from a developer's perspective, focusing on security, data modeling, and usability. DDS offers dynamic network topology and rich QoS policies, ideal for industrial settings. MQTT emphasizes small code footprint and low network bandwidth. VSL provides logic-data separation and explicit data modeling. A rating table aids in informed protocol selection, considering project requirements. This analysis guides IoT architects in selecting the most suitable middleware for specific use cases.

In 2019, Tanushree Agarwal, Payam Niknejad, M. R. Barzegaran1, Luigi Vanfretti [8] it presents a Multi-level Time Sensitive Networking (TSN) protocol utilizing Data Distribution Service (DDS) middleware for real-time transfer of synchronized three-phase measurement data. The protocol ensures low latency and packet loss by prioritizing data and shaping network traffic through Quality of Service (QoS) profiles. Implemented with the RTI Connext framework and MATLAB classes, the protocol offers granular control over traffic shaping and scheduling, making it suitable for time-critical applications in microgrids, smart cities, and military settings. Real-time testing validates its effectiveness in handling ultra-fast sampled data securely with satisfactory performance in latency and throughput parameters.

In 2017, Ruben Cruz Huacarpuma, Rafael Timoteo de Sousa Junior, Maristela Terto de Holanda, Robson de Oliveira Albuquerque, Luis Javier García Villalba, and Tai-Hoon Kim. [6] introduces a Distributed Data Service (DDS) tailored for IoT environments, aiming to facilitate data collection and processing across multiple middleware systems. The DDS specification includes functionalities for data collection, filtering, and storage, alongside a data aggregation component for real-time querying. Case studies evaluating DDS performance in simulated smart home systems demonstrate its efficacy compared to existing

middleware like UIoT and Kaa. This research underscores the importance of effective database middleware technology in managing the massive volumes of real-time data generated by IoT devices, positioning DDS as a promising solution for collaborative data treatment in diverse IoT environments.

In 2012, Kai Beckmann and Marcus Thoss Distributed Systems Lab [7] proposed "Wireless Sensor Network Protocol for the OMG Data Distribution Service". It proposes SNPS, an alternative transport protocol for the OMG Data Distribution Service (DDS), aimed at wireless sensor networks (WSNs). While DDS is a promising standard for WSNs, its reliance on resource-intensive protocols like RTPS poses challenges. SNPS, designed for highly resource-constrained sensor node platforms, offers a solution by focusing on low-powered hardware and small frame sizes. It ensures interoperability while supporting a reasonable feature set of the DDS standard, making it suitable for WSN architectures.

IV. PROPOSED SYSTEM:

This section outlines the architecture of the envisioned home automation system developed throughout the research project, detailing the systematic approach and design phases. Initially, the system's main components are highlighted, accompanied by diagrams illustrating the communication infrastructures they utilize. Each component is succinctly elucidated within distinct subsections. Subsequently, the analysis and design criteria resulting from the project's analysis phase, which informed the implementation phase, are enumerated from the perspective of the system designers. The ongoing implementation of the system is then briefly assessed against these criteria.

A. System Architecture

The basic infrastructure design as a top-view is given in Fig. 1.

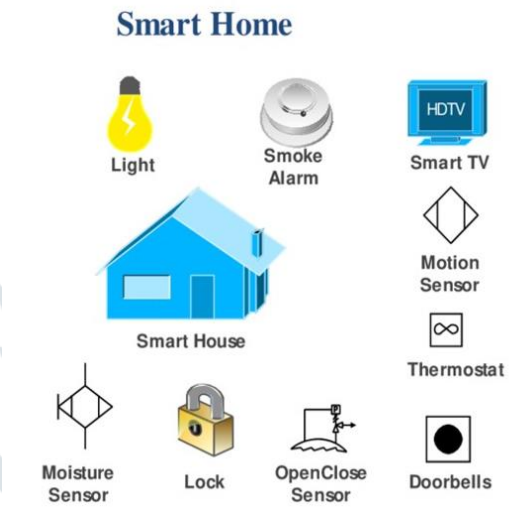

Fig. 1. Infrastructure and few components of a smart home.

The infrastructure mainly compresses of two components: local hardware, and middleware. But a mobile smart device can be implemented in further days as the third component. The local hardware comprises the whole and soul of the network, i.e., the server and client sensors. The server is built up using Raspberry Pi and the various environment sensing sensors act as client nodes. While the use of DDS and UPD is seen for middleware prototyping.

1) Local hardware

Raspberry Pi Model 4B, 4GB RAM, in-built 2.4/5GHz Wireless and Bluetooth 5.0 and ARMv8 processor, servers as a server in this infrastructure. It consists of a SD slot underneath the printed circuit board, embedded with components. A SD card is formatted and necessary software is flashed into the disk. Which is then inserted into the slot, to boot and configure the OS on the hardware. The Raspberry Pi is equipped with two USB ports (i.e., USB 2.0 and USB 3.0) to connect keyword and mouse for navigation and data entry. It also consists of micro-HDMI ports for display use, CSI camera and display ports for installation of camera and a display unit respectively. The in-built 2.4/5GHz Wireless and Bluetooth 5.0 servers as our communication medium.

Fig. 2. Raspberry Pi Model 4B

The Raspberry Pi chip can record and updated data to its session. The chip is bootable from micro SD card, and is a duplex communication mode based device (i.e., the ability to send/ receive data and information between appliances and server). This device has characteristics as capable as a simple computer with embedded components. The suggested system could utilize a Raspberry Pi for orchestrating home appliance management. The data retrieved during the session is transmitted from the local device to its serial port, where it interfaces with a controller. While various types of controllers could be employed, the envisioned system opts for an ARM controller for direct oversight of household appliances. The initial implementation includes an alarm linked to a smoke sensor, a lamp activated by automatic switches managed through a home automation app, and an air-conditioner monitoring home climate adjustment. Additional household devices can be seamlessly integrated into the system as required.

2) Middleware

In this prototype of home automation demonstration, we prefer to utilize Data Distribution Service (DDS) as the primary middleware for setting up of server and client. The Data Distribution Service (DDS) is a specification for distributed systems based on the publish-subscribe paradigm published by the Object Management Group (OMG), DDS applications efficiently share data across the network using strongly-typed and asynchronous cache updates based on topics and QoS policies. Data-Centric Publish-Subscribe (DCPS) is the application model defined by the DDS specification. This section describes the main concepts and entities of the DCPS API and how they interact and work together.

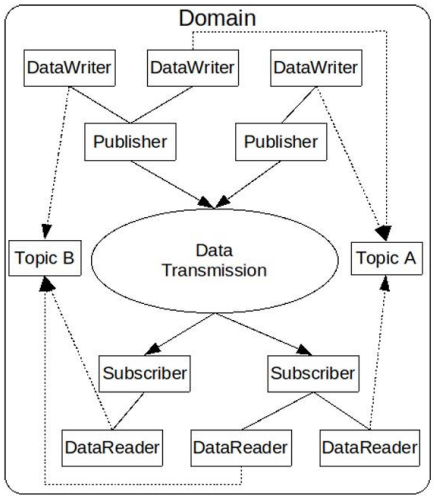

Fig. 3. DCPS Conceptual Overview

The main concept that is drawn from Fig. 3 is the publisher and subscriber. In the realm of publishing and subscribing applications, the cornerstone of interaction lies in the distinct channels that bridge publishers and subscribers. Each channel is uniquely identified within the domain, facilitating the seamless connection between publishers and subscribers. This framework allows for a multitude of processes to publish to a given channel, and likewise, numerous processes can subscribe to the same channel, fostering a dynamic many-to-many communication paradigm. When a publishing process transmits samples, it designates the specific channel through which they are disseminated. Conversely, a subscribing process solicits samples by specifying the desired channel, thus orchestrating a coherent exchange of information within the system.

A publisher assumes the crucial responsibility of distributing published data to all pertinent subscribers across the domain. The specific method utilized for this dissemination is determined by the implementation of the service. Participants within the system may be associated with multiple publishers, and each publisher may in turn manage multiple data writers, potentially across diverse topics. Publishers possess the capability to consolidate a sequence of writes spanning multiple data writers, presenting it to subscribers as a cohesive modification.

On the other hand, a subscriber receives data from the publisher and directs it to any relevant data readers under its purview. Participants within the ecosystem can accommodate multiple subscribers, with each subscriber potentially overseeing multiple data readers across varied topics.

Transmission of samples and information related to their management is accomplished via an Open DDS-specific transport framework that allows the service to be used with a variety of transport protocols. Transports are typically specified via configuration files and are attached to various entities in the publisher and subscriber processes. Fig. 4 shows how the transportation in OpenDDS occurs.

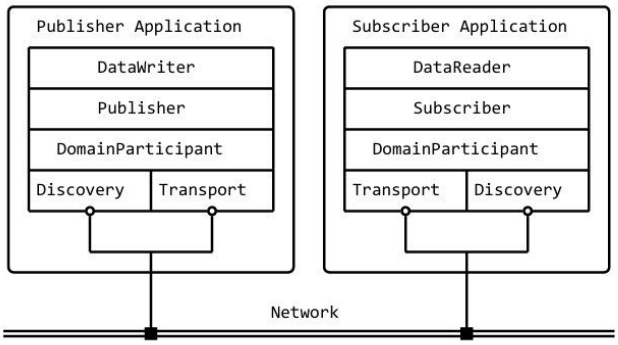

Fig. 4. OpenDDS communication framework

The transports are of few types namely, TCP Transport, RTPS/UDP Transport, Multicast Transport, Shared Memory Transport and Custom Transport. The work utilizes UDP transport which uses unicasted UDP as the transmission mechanism.

B. System Analysis and Evaluation

During the initial phases of the project, the analysis and design stages focused on determining the key criteria for an efficient home automation system. This involved a collaborative effort among the project team members to simulate the end-user experience and identify desired functionalities. The analysis began with the core team members, representing different user perspectives, envisioning the requirements for an office or home automation system.
Drawing from these discussions and expert insights, a comprehensive list of criteria essential for a robust home automation system was compiled. It's important to note that while these criteria reflect the viewpoints of the project team, they are informed by rigorous requirement analysis mechanisms and aim to align with state-of-the-art technologies.
The evaluation of the prototype system, which employs Wi-Fi modules for communication, Raspberry Pi as the hardware platform, and DDS and UDP as middleware, was conducted in accordance with the established criteria. Through extensive testing with various users and sub-users, the system's performance was assessed against standard criterion. This serves as a comprehensive guide for assessing the effectiveness and suitability of the implemented home automation system, and ensures that the system meets the requisite standards of functionality, reliability, and user satisfaction within the specified technological framework.

V. CONCLUSIONS:

IoT-based home automation system represents a significant advancement in smart home technology, offering homeowners unprecedented control, convenience, and efficiency in managing their living spaces. By leveraging Raspberry Pi, ESP8266 boards, and UDP communication protocol, the system demonstrates the potential of IoT technologies to revolutionize home automation and improve quality of life. Moving forward, continued research, innovation, and collaboration will be essential to overcome challenges, enhance functionality, and realize the full potential of IoT-enabled smart homes. In this comprehensive literature review, we have explored the design and implementation of an IoT-based home automation system utilizing Raspberry Pi as the central server, ESP8266 boards for device integration, and UDP (User Datagram Protocol) as the communication protocol. By integrating a diverse range of sensors, actuators, and functionalities, the system offers homeowners enhanced control, convenience, and efficiency in managing their household appliances and environmental conditions.

VI. REFERENCES:

[1] "A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes", Arya Yudidharmaa, Nicholas Nathaniela, Tang Nyquel Gimlia, Said Achmada, Aditya Kurniawan.

[2] "Design and Implementation of a Framework for Smart Home Automation Based on Cellular IoT, MQTT, and Serverless Functions", Marco Esposito, Alberto Belli, Lorenzo Palma and Paola Pierleoni.

[3] "A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications", Vasilios A. Orfanos, Stavros D. Kaminaris, Panagiotis Papageorgas , Dimitrios Piromalis and Dionisis Kandris.

[4] "Wireless Communication Without Internet Connection", Abeye Tewodros, Ananya Samuel, Ebenezer Mulugeta, Nawid Barakzai, Sal Sabila Kouser, Dr. Vijay Kumar.

[5] “DDS vs MQTT vs VLS”, Georg Aures, Christian Lübben.

[6] “Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer”, Tanushree Agarwal, Payam Niknejad, M. R. Barzegaran1, Luigi Vanfretti.

[7] Ruben Cruz Huacarpuma, Rafael Timoteo de Sousa Junior, Maristela Terto de Holanda, Robson de Oliveira Albuquerque, Luis Javier García Villalba, and Tai-Hoon Kim proposed “Distributed Data Service for Data Management in Internet of Things Middleware”.

[8] “Wireless Sensor Network Protocol for the OMG Data Distribution Service”, Kai Beckmann and Marcus Thoss Distributed Systems Lab.