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

SafeConnect IoT Shield

[1]Prof.Leena Patil Author,[2]Akash Chintakindi,[3]Harshda Khairnar,[4]Sahil Pawar

[1]Professor, [2]Student, [3]Student,[4]Student
Dept. of Electronics & Telecommunication
Xavier Institute of Engineering ,Mumbai, India

Abstract : The Internet of Things (IoT) landscape, characterized by its expansive growth across sectors, presents unprecedented opportunities for connectivity and automation but simultaneously exposes critical vulnerabilities, necessitating robust security frameworks. This paper introduces the CyberShield IoT project, a pioneering initiative designed to address the multifaceted security challenges inherent in interconnected devices, networks, and ecosystems. With a primary objective to enhance IoT security paradigms, CyberShield focuses on developing a fortified IoT model equipped with advanced encryption, authentication, and access control mechanisms. Leveraging real-time threat detection algorithms and machine learning capabilities, the project aims to monitor, analyze, and respond to malicious activities, breaches, and attacks promptly, ensuring data integrity, system resilience, and user trust. By synthesizing innovative approaches and best practices, CyberShield endeavors to propel IoT security beyond current limitations, fostering a secure, reliable, and resilient IoT landscape capable of navigating and neutralizing evolving cyber threats, vulnerabilities, and challenges, thereby contributing to the advancement of IoT security research, development, and innovation.

IndexTerms **- Internet of Things (IoT), CyberShield IoT project, security frameworks**

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has heralded transformative changes across diverse sectors, ranging from healthcare and transportation to agriculture and smart cities, by facilitating unparalleled connectivity, automation, and data-driven insights. While this proliferation promises unprecedented opportunities for innovation and efficiency, it concurrently amplifies significant security challenges, spotlighting concerns surrounding data privacy, system integrity, and protection against an array of evolving cyber threats and malicious activities. Amidst this backdrop, the CyberShield IoT project emerges with a pivotal objective: to craft a novel and secure IoT framework tailored to safeguard interconnected devices, networks, and ecosystems.

By anchoring its focus on developing a fortified IoT model fortified with robust encryption, authentication, and access control mechanisms, CyberShield endeavors to fortify sensitive data against unauthorized access, tampering, and exploitation. Concurrently, the project integrates cutting-edge real-time threat detection algorithms and anomaly identification techniques, harnessing the power of machine learning to monitor, analyze, and counteract malicious activities and breaches promptly.

In synthesizing these innovative approaches, CyberShield aspires not only to address the existing security lacunae but also to propel IoT security paradigms beyond contemporary limitations, fostering a resilient, trustworthy, and secure IoT landscape poised to navigate and neutralize evolving cyber threats, vulnerabilities, and challenges.

II. OBJECTIVES

The objective is to develop a secure IoT model with a protected server, encrypted client-server communication. Implement real-time threat detection to identify and respond to external breaches, ensuring data integrity and system safety. Design an automated shutdown mechanism for com-promised clients to prevent further network vulnerability and unauthorized access.

III. LITERATURE REVIEW

In our research for this project, we looked at many IEEE papers to understand the latest trends and methods in our field. These papers were crucial because they gave us important insights into various techniques, advancements, and concepts that shaped our project. By studying these trusted sources, we aimed to make our approach more robust and credible, aligning our work with well-established research practices. The information from these papers helped us understand the current state of research better and provided ideas that influenced our project's direction and innovation.

Paper Title	Authour	Year	Summary	Advantages	Disadvantages
Design and Implementation of Raspberry House: An IoT Security Framework	Wen Fei	2021	A Raspberry Pi within an Ethernet network can be used as a wireless access point by creating a private network. The resulting new wireless network is entirely managed by Raspberry Pi.	Comprehensive Device Security, Early Threat Detection, Data Privacy Assurance	Maintenance Overhead, Compatibility Challenge
A Survey on Security Attacks and Solutions in the IoT Network	Xingwei Liang	2021	Potential IoT solutions encompass edge computing, machine learning, and blockchain.	Enhanced Security, Data Efficiency	Complexity, Scalability
Raspberry pi based secured cloud data	Cheng-Ying Yang	2021	The system employs a hard disk connected to a Raspberry Pi running OpenMediaVault OS. Accessible within the network.	Data Control, Accessibility, Security	Hardware Dependency, Performance

Paper Title	Authour	Year	Summary	Advantages	Disadvantages
Research on Information Security Protection Technology of Client Side System	Bin Yang	2020	The research focuses on improving security for client-side energy systems by employing a trusted encryption approach based on the AES-DES algorithm with chaos	Proposed security approach for client-side energy control systems include enhanced protection	Challenges include complex implementation, potential processing overhead
Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform	Ghawar Said	2022	It defines the components of smart home systems, discusses essential safety aspects like fire and gas leakage, and emphasizes wireless communication methods.	Real-time monitoring, remote control, automation	High costs, privacy worries, vulnerability to hacking

Paper Title	Authour	Year	Summary	Advantages	Disadvantages
Design and Implementation of Raspberry House: An IoT Security Framework	Wen Fei	2021	A Raspberry Pi within an Ethernet network can be used as a wireless access point by creating a private network. The resulting new wireless network is entirely managed by Raspberry Pi.	Comprehensive Device Security, Early Threat Detection, Data Privacy Assurance	Maintenance Overhead, Compatibility Challenge
A Survey on Security Attacks and Solutions in the IoT Network	Xingwei Liang	2021	Potential IoT solutions encompass edge computing, machine learning, and blockchain.	Enhanced Security, Data Efficiency	Complexity, Scalability
Raspberry pi based secured cloud data	Cheng-Ying Yang	2021	The system employs a hard disk connected to a Raspberry Pi running OpenMediaVault OS. Accessible within the network.	Data Control, Accessibility, Security	Hardware Dependency, Performance

IV. Limitations of Existing system

Many existing IoT systems lack robust security measures, relying on basic encryption and authentication methods. This inadequacy leaves them vulnerable to sophisticated attacks, including intrusion, data breaches, and device manipulation. IoT networks consist of a wide array of devices, each with unique specifications and communication protocols. Existing solutions often struggle to provide uniform security across this diverse ecosystem, leading to vulnerabilities in certain devices or communication channels.

V. Problem Statement

"Developing CyberShield IoT: a novel security framework that ensures end-to-end protection of IoT connections, detecting and blocking external breaches, and enabling automatic shutdown in case of client compromise, thus advancing IoT security beyond current solutions."

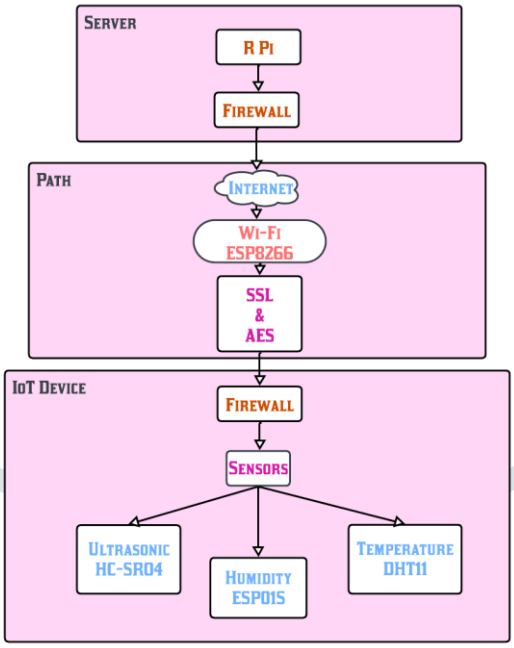
VI. Research Methodology

The establishment of a secure IoT ecosystem involves a systematic series of steps beginning with the setup of the Raspberry Pi as the central server and the configuration of STM Boards as clients, each integrated with various sensors. Network security is fortified through the installation and configuration of a firewall on the Raspberry Pi, meticulously allowing only authorized communication channels between the server and clients. The implementation of SSL/TLS protocols ensures the encryption of communication, guaranteeing data authenticity and confidentiality. To bolster defense against potential threats, an Intrusion Detection System (IDS) is deployed on the server, equipped with rules and algorithms designed to detect suspicious patterns and behaviors. Automated scripts are then developed to initiate the swift shutdown of compromised clients upon detection, preventing unauthorized access and potential data manipulation. The secure connection of sensors precedes the implementation of local data processing algorithms on the boards, ensuring the integrity of the collected data. This processed data is then securely transmitted to the central server via encrypted channels, upholding end-to-end security. Finally, the development of a user-friendly dashboard enables real-time monitoring of connected devices, security alerts, and overall system health, fostering an intuitive and accessible interface for users to engage with the IoT network effectively. This comprehensive approachnot only ensures the seamless integration of IoT components but also establishes a resilient and user-centric security framework suitable for various applications.

3.1Framework:

In this comprehensive IoT security framework, a Raspberry Pi server serves as the central hub, orchestrating and securing the entire network. The server hosts a robust firewall, meticulously configured to monitor and regulate both incoming and outgoing network traffic, allowing only authorized communication between the server and the IoT devices, represented by STM Boards. SSL/TLS encryption protocols are employed to establish secure channels, ensuring the authenticity and confidentiality of data exchanged between the server and clients through SSL certificates. To enhance network security, an Intrusion Detection System (IDS) is implemented on the server, equipped with predefined rules and machine learning algorithms to detect suspicious patterns and potential external threats. In the event of a security breach, an automatic shutdown mechanism triggers, swiftly isolating compromised clients to prevent further unauthorized access and potential data manipulation. The IoT devices, equipped with various sensors such as temperature, motion, and humidity sensors seamlessly integrate into the network. These sensors collect environmental data, undergo secure processing via client-side algorithms, and transmit the information securely to the server, maintaining data integrity and authenticity through SSL encryption. A user-friendly web or mobile application, the User Dashboard, is developed to provide users with a seamless interface for monitoring connected devices, security alerts, and overall system health

in real-time. This holistic approach not only ensures the secure functioning of the IoT network but also facilitates user engagement through efficient monitoring and alert mechanisms.



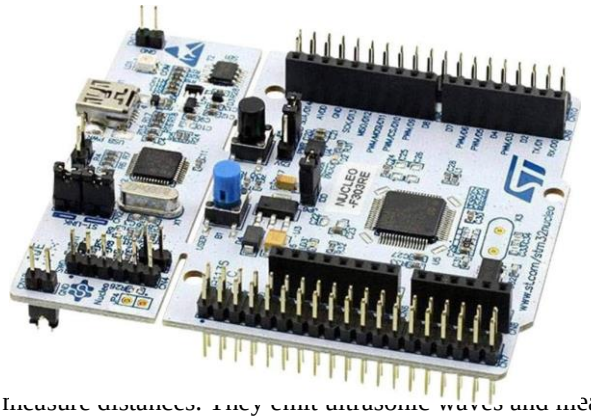
3.2 HARDWARE Used

A. Raspberry Pi

Foundation is a British company that developed the Raspberry Pi line of tiny single-board computers. Owing to its small size and adaptable features, it is utilized in many applications, including Internet of Things initiatives.It is used in various applications, including IoT projects, due to its compact size and versatile capabilities. applications, including IoT projects, due to its compact size and versatile capabilities.

B. STM32:

A family of microcontroller units (MCUs) produced by STMicroelec-tronics. These microcontrollers are widely used in embedded systems and IoT projects due to their reliability and performance.



C. Ultrasonic sensors:

Are devices that use sound waves to measure distances. They emit ultrasonic waves and measure the time it takes for the waves to bounce back after hitting and object, allowing for distance calculation.

.

D. Humidity sensors:

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR sensors are commonly used in security alarms and automatic lighting applications..

3.3 SOFTWARE Used

A. MongoDB

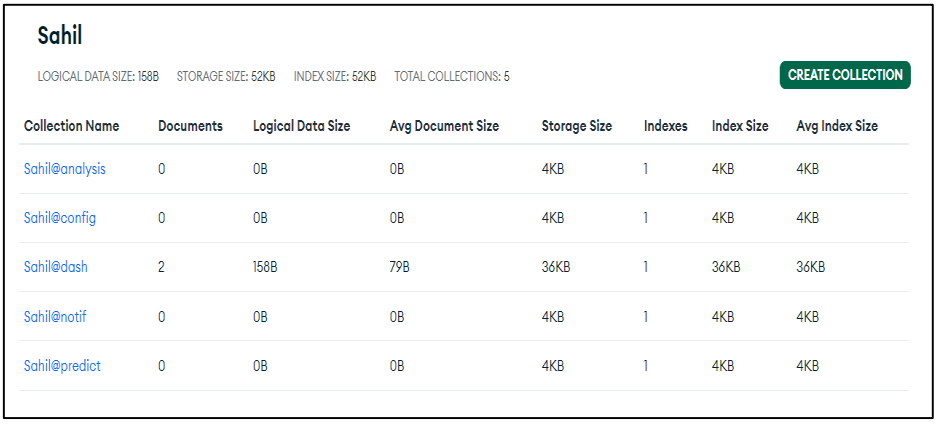
MongoDB, an open-source NoSQL database, offers high performance, availability, and scalability. It's Document-oriented approach utilizes flexible BSONdocuments, accommodating diverse data types. With a dynamic schema, MongoDB allows easy document structure modification. It boasts a robust query language, horizontal scalability through sharding, and an aggregation framework for advanced data processing. Ensuring high availability, MongoDB supports replica sets, and the company MongoDB,Inc, provides professional support for enterprises using it in production environments.

B. PageKite

PageKite empowers users to expose local servers or websites to the internet without a public IP or intricate firewall setup. Utilizing reverse proxying, it connects servers to the PageKite service, providing accessibility via custom domain names. Supporting HTTP, HTTPS, SSH, and more, PageKite ensures secure service exposure with encryption and authentication. With dynamic DNS and open-source flexibility, it's a go-to for dynamic IP scenarios. Users configure it through the command line or a file, making it ideal for developers and small businesses seeking cost-effective hosting solutions.

VII. RESULT AND DISCUSSION

Here are the results of our first implementation for our project "Data Shielding in IoT Network of a Warehouse " For the first phase of our project we successfully installed and configured Nextcloud as our Personal self-hosted cloud as a Server on a Raspberry Pi.



Sahil

LOGICAL DATA SIZE: 158B STORAGE SIZE: 52KB INDEX SIZE: 52KB TOTAL COLLECTIONS: 5

CREATE COLLECTION

Collection Name	Documents	Logical Data Size	Avg Document Size	Storage Size	Indexes	Index Size	Avg Index Size
Sahil@analysis	0	0B	0B	4KB	1	4KB	4KB
Sahil@config	0	0B	0B	4KB	1	4KB	4KB
Sahil@dash	2	158B	79B	36KB	1	36KB	36KB
Sahil@notif	0	0B	0B	4KB	1	4KB	4KB
Sahil@predict	0	0B	0B	4KB	1	4KB	4KB

Fig.10.1 Result

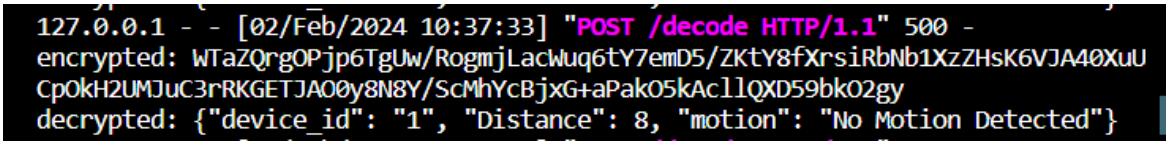


Fig. 10.2 Result

VIII. CONCLUSION AND FUTURE SCOPE

Our CyberShield IoT project, we successfully implemented a secure server using Raspberry Pi,Python, and Visual Studio Code, enabling real-time data access locally and on other devices. This achievement establishes a strong foundation for advancing our project, emphasizing its feasibility, scalability, and potential for robust IoT connection safeguarding in subsequent phases. Moving forward, we will focus on enhancing security protocols and user experience to create a comprehensive and reliable IoT solution.

The future scope of the CyberShield IoT project includes enhancing security features, expanding device compatibility, integrating machine learning for intelligent data analysis, enabling remote management through mobile applications.

REFERENCES

[1] Bin Yang , Xuesong Shao “Research on Information Security Protection Technology of Client Side System” 2020 Chinese Automation Congress (CAC) IEEE, DOI:10.1109/CAC51589.2020.9327122.

[2] Ghawar Said,Anwar Ghani,AtaUllah,Muhammad Azeem,Muhammad “Systematic Survey on Smart HomeSafety and Security Systems Using the Arduino Platform” 2022 Korean Government [Ministry of Science and ICT (MSIT)] DOI 10.1109/AC-CESS.2020.3008610

[3] Anyi Liu,Ali Alqazzaz,Hua Ming,Balakrishnan Dharmalingam, “Iotverif: Automatic Verification of SSL/TLS Certificate for IoT Applications”, 2021 National Science Foundation of the United States under Grant No. DGE-1723707 and in part by NASA, DOI:10.1109/ACCESS.2019.2961918.

[4] Ghawar Said,Anwar Ghani,Ata Ullah,Muhammad Azeem,Muhammad Bilal,Kyung Sup Kwak “Light-Weight Secure Aggregated Data Sharing in IoT-Enabled Wireless Sensor Networks” , 2022 National Research Foundation of Korea-Grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant NRF-2020R1A2B5B02002478, DOI: 10.1109/ACCESS.2022.3160231.

[5] Hariprasad Siddharthan,T. Deepa,Prabhu Chandhar, “SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features” , 2022 SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu 603203, India , DOI: 10.1109/ACCESS.2022.3161566. .

[6] Wen Fei, Hiroyuki Ohno, Srinivas Sampalli, “Design and Implementation of Raspberry House: An IoT Security Framework” 2021,IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)IEEE, DOI:10.1109/IoTaIS50849.2021.9359722,ISBN:978-1-7281-9449-3

[7] Xingwei Liang,Yoohwan Kim, “A Survey on Security Attacks and Solutions in the IoT Network” 2021,IEEE E 11th Annual Computing and Communication Workshop and Conference (CCWC) , DOI:10.1109/CCWC51732.2021.9376174

[8] Cheng-Ying Yang, Cheng-Chi Lee, TsueiHung Sun et al. , “Raspberry pi based secured cloud data” 2021,IEEE Journal of Physics: Conference Series ,DOI 10.1088/1742-6596/1964/4/042101