A Secure and Energy-Efficient Cross-Layer Framework for Internet of Things

Rashid Mustafa
Computer Science and Software Engineering
Auckland University of Technology
Auckland, New Zealand
rashid.mustafa@autuni.ac.nz

Nurul I Sarkar
Computer Science and Software Engineering
Auckland University of Technology
Auckland, New Zealand
nurul.sarkar@aut.ac.nz

Mahsa Mohaaghegh
Computer Science and Software Engineering
Auckland University of Technology
Auckland, New Zealand
mahsa.mohaghegh@aut.ac.nz

Shahbaz Pervez
Department of Information Technology
Whitecliffe College of Art and Design
Auckland, New Zealand
shahbazp@whitecliffe.ac.nz

Abstract:.This study addresses the problem of maximizing the power consumption of IoT (Internet of Things) devices while protecting them against cyberattacks. A layered architecture can be useful for addressing the unique challenges of security and energy efficiency in IoT systems. To this end, we propose a secure and energy-efficient cross-layer framework for IoT applications. The proposed cross-layer framework is based on collaboration among physical (sensor), network, and application layers. We examine the need for a three-layered approach in achieving the balance between security and energy efficiency. The proposed approach aims to provide a major leap in the areas of security and energy efficiency in IoT deployments. The system performance is validated by test-bed measurements with a focus on resource-constrained IoT settings. Using Cooja simulator we assess application-layer vulnerabilities and energy efficiency. The findings reported in this paper provide some insights into the design and deployment of IoT systems using a cross-layer design approach.

Keywords: Cross-layer framework, Energy-efficient, IoT (Internet of Things), Security

I. INTRODUCTION

The Internet of Things (IoT) has rapidly grown into the largest computing platform, connecting processes, data, and people[1]. It facilitates both machine-to-machine and people-to-people communication. Cyber-Physical Systems (CPS) have gained popularity, focusing on embedded intelligent systems such as controllers, sensors, and actuators [2]. CPS is known for its dependability and efficiency. However, managing IoT devices and applications poses challenges, with varying programming complexity and significant battery power consumption. To address this, the development of a resource-efficient communication protocol to enforce IoT device sleep mode when idle is crucial to save battery power.

Energy efficiency in computing devices and technologies for low-power residential and commercial buildings has raised concerns. Research has delved into specific applications related to heating systems' energy efficiency, investigating hardware and software control mechanisms and the use of historical data for energy consumption forecasts [3]. The analysis revealed application-specific variables that must be considered for planning, recommending the use of wireless low-power sensors on a larger scale and the importance of security against eavesdropping attacks.

Blockchain technology is proposed to enhance secure vehicular communication, ensuring that only trustworthy vehicles participate while addressing various security concerns [4]. The growing cost and complexity of cybercrime emphasize the need for new procedures, tools, and public awareness. The constantly changing threat landscape necessitates annual reviews of tools and procedures to adapt to evolving risks.

In this paper, we address the following research question.

What secure and energy-efficient cross-layer framework can be developed for IoT?

To answer the question posed we propose a cross-layer energy-efficient framework for secure IoT applications. This framework aims to provide data integrity, confidentiality, availability, and privacy across multiple layers and address energy efficiency concerns. The key contributions of this paper are highlighted below.

a) Developing a Secure Protocol for Enhanced IoT Framework Security.

Creating a safe Internet of Things protocol with a focus on secure communication, integrity, authentication, and encryption for linked devices. making adherence to standards, privacy, network security, and comprehensive documentation a priority. Goal: strengthen the security of the IoT framework to guarantee data availability, confidentiality, and integrity while fostering ecosystem growth.

b) Creating an Energy-Efficient Protocol for Improved IoT Framework Efficiency

Developing an energy-efficient protocol to enhance resource usage and reduce energy consumption to maximize the efficiency of the Internet of Things architecture. A protocol centred on energy efficiency is intended to improve the performance and sustainability of Internet of Things systems.

As IoT devices expand, energy efficiency and security are paramount concerns. Traditional layered architectures may not fully address these issues, prompting the development of cross-layer frameworks. These frameworks optimize communication and processing across layers to reduce energy usage and enhance security by combining security procedures and intelligence across multiple layers.

The framework's significance lies in addressing IoT-specific security risks, promoting energy-efficient algorithms, ensuring compatibility and interoperability, scalability, and supporting environmentally friendly practices. It safeguards IoT systems, extends device lifespans, and fosters innovation in various industries. The cross-layer architecture promotes a more efficient and secure IoT ecosystem, aligning with environmental objectives and expanding the range of IoT applications and services. The reason for the research and similar works are discussed at the Section II and explores the background and a review of the literature. The suggested architecture is shown in Section III. A summary of the findings and debate may be found in Section IV. Section V offers the conclusion at the end. The research motivation and related work is discussed next.

II. Motivation and Related Work

The main focus of this research is to improve service quality in terms of security and energy efficiency aspects of IoT. Layer-to-layer jumping is possible due to the data flow between node layers [5]. A protocol establishes how data is transferred between levels. Traditional network layers are outperformed by cross-layered techniques. Future location-based routing protocols could be used to exchange battery data between the physical and MAC layers are known as Perception-Layer. To improve energy efficiency, the proposed routing protocol and a cross-layer technique were used.

IoT is a technological advancement that is revolutionizing how we work, play, and communicate. Faced various difficulties with regard to storage, bandwidth, finite power, and processing power [6]. For devices to stay connected to the network for an extended period, the issue of constrained battery-operated devices must be solved. During packet transmission and reception, IoT devices use energy. If energy efficiency is considered, reliable transmission presents a significant challenge. When sending packets from source to destination, a routing protocol is essential. It is crucial to assess a routing protocol appropriate for IoT devices with limited power. RPL (Routing protocol for low power and lossy networks) and LOADng (Lightweight on-demand Ad-hoc distance vector routing protocol next generation) are compared in this article. This study assessed the networked power usage of IoT devices. The Contiki operating system and the Cooja Network Simulator are used to evaluate the protocols. RPL is an effective protocol for energy efficiency, according to the outcome.

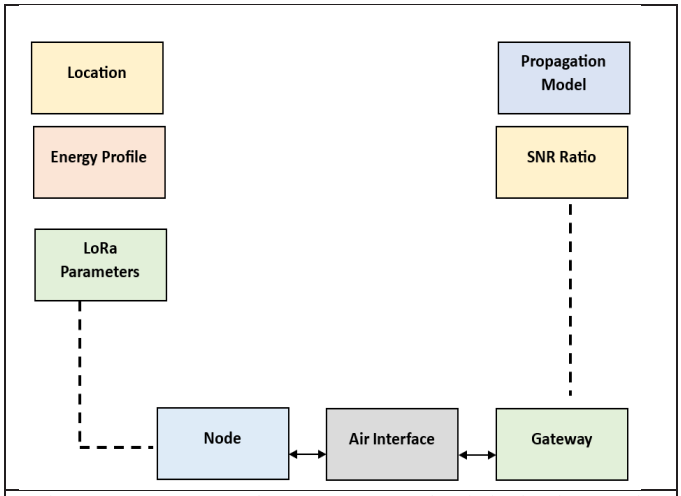

Figure 1. LPWAN Cross-layer assessment and optimization framework

The review of the literature reveals that dynamic reduced round cryptography, lightweight on-demand ad-hoc distance vector routing protocol, and routing protocol for low power lossy networks are all used for energy efficiency and have already been put to the test in the network layer [7].The practices and protocol mentioned above can be adapted for use in other layers of our suggested architecture. In doing so, one can increase the energy efficiency of devices with limited energy.

Research covers IoT introduction, security requirements, and case studies, highlighting the need to protect customer privacy and address security issues [8].

Cyber threats to sensor devices are a focal point, including data and network attacks across various layers. Proposed solutions involve middleware security and machine learning algorithms [9]. The strategy for defending IoT environments includes continuous monitoring and testing during development to counter various threats. A smart detection system based on intelligent architectural frameworks addresses network security and privacy concerns.

The physical layer and MAC-layer, both affect how autonomous IoT devices are. Low power wide area networks (LPWANs) were given a cross-layer assessment framework. Recent energy models, download messages, and adaptive data rate features were also covered [8]. Testing and analysis of transmission schemes and hypotheses. It also evaluated one of the LoRaWAN protocol's test cases (Fig. 1). The discovery help to direct the effective use of LPWANs in terms of throughput and energy efficiency. Various experiments are used to evaluate the cross-layer approach. By enhancing channel dynamics and packet length, energy efficiency can be attained.

The focus of the work is on low-speed, long-range IoT networks with a significant number of IoT sensors. The periodically repeated communication involves using a transmission slot for transmission. Only one IoT device is allowed to send data during each slot. The proposed three-layed IoT architecture and the corresponding OSI layer is shown in Fig. 2.

Proposed Architecture	OSI Architecture	Protocols/ Methods
Application Layer	Application Layer	Lightweight Symmetric Cipher
	Presentation Layer	
Network Layer	Session Layer	Dynamic Redudced Round Cryptography, NB-IoT, & LoRaWAN, LOADng, Mary Modulation
	Transport Layer	
	Network Layer	
	Datalink Layer	Resolving data collision
Sensor Layer	Physical Layer	Nothing found for Sensor Layer

Figure 2. Comparison of proposed three-layed IoT architecture with OSI architecture

The necessity of security in IoT networks is emphasized by the authors as they addressed the IoT's explosive growth and the related security issues. It proposes software-defined security and discusses cyber-physical system security [9]. The challenges of the 2020 pandemic and the increased number of IoT attacks are also addressed [10]. The importance of secure cybersecurity architecture is highlighted, with a focus on mitigating weaknesses like weak passwords, insider threats, and external attacks.

The IoT cross-layer frameworks research field aims to optimize network performance and energy usage within IoT ecosystems by improving communication protocols and integrating multiple layers. The goal is to extend device battery life, reduce environmental impact, and ensure seamless interoperability, scalability, and strong security. Data security is a significant concern, particularly with the exponential growth of IoT.

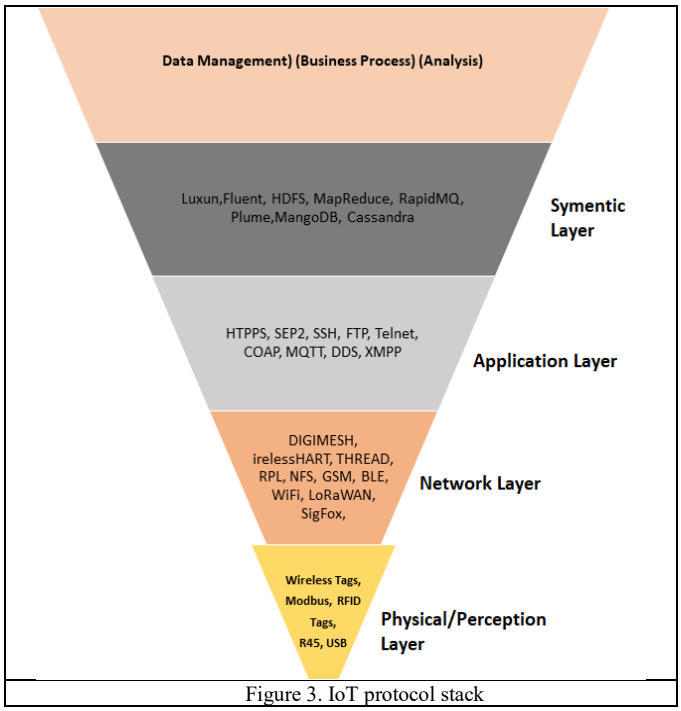

Figure 3. IoT protocol stack

We highlight the necessity of ongoing awareness and flexibility in the ever-changing landscape of cybersecurity. Finally, we support the use of many layers of protection and particular security mechanisms in IoT architecture. Networks that use less energy are crucial, as is energy saving via better routing and power management. The research methodology involves simulation and testing, emphasizing the need for cross-layer routing protocols to improve energy efficiency and secure architecture for IoT applications. It also aims to identify and prioritize security objectives, assess potential threats, and select appropriate security controls. Real-world testing and security analysis are crucial for validating the proposed architecture's security measures.

The justification for this secure and energy-efficient architecture includes reliability, resource optimization, cost savings, environmental sustainability, and improved user experience. Energy efficiency metrics and performance metrics are discussed to optimize resource utilization and ensure the confidentiality and integrity of patient data and healthcare systems. Additionally, it provides a thorough research methodology for assessing and putting into practice a cross-layer framework that is both secure and energy-efficient for Internet of Things applications in the healthcare industry and other fields. The effectiveness of the suggested architecture is measured and validated primarily through the use of security and energy-efficiency metrics.

III. Proposed Cross-Layer Framework

A layered architecture is essential for addressing the unique challenges of security and energy efficiency in IoT systems. This approach involves examining each layer of the IoT system, from physical to application layers, to identify vulnerabilities and inefficiencies. The interplay between security and energy efficiency is crucial, making a cross-layer approach vital. Security measures should span multiple layers and include access control, secure communication protocols, anomaly detection tools, and encryption/authentication mechanisms. Simultaneously, energy optimization techniques, like low-power device design and adaptive transmission, must be explored across various layers. The aim of frameworks that combine cybersecurity with energy efficiency is to build a robust and sustainable basis for IoT ecosystems by optimizing energy use and mitigating cybersecurity risks.Testing and performance metrics are used to assess the impact of cross-layer architectures on security and energy efficiency, with iterative improvements based on testing feedback.

System Architecture: The architecture is designed to efficiently manage user requests related to new technological advancements as shown in Fig. 4. It consists of three layers: the Application Layer, Network Layer, and Sensing Layer. Each layer is equipped to perform specific tasks that streamline the process of fulfilling user requests for resources. This architecture aims to enhance the user experience and the efficiency of resource allocation for emerging technologies.

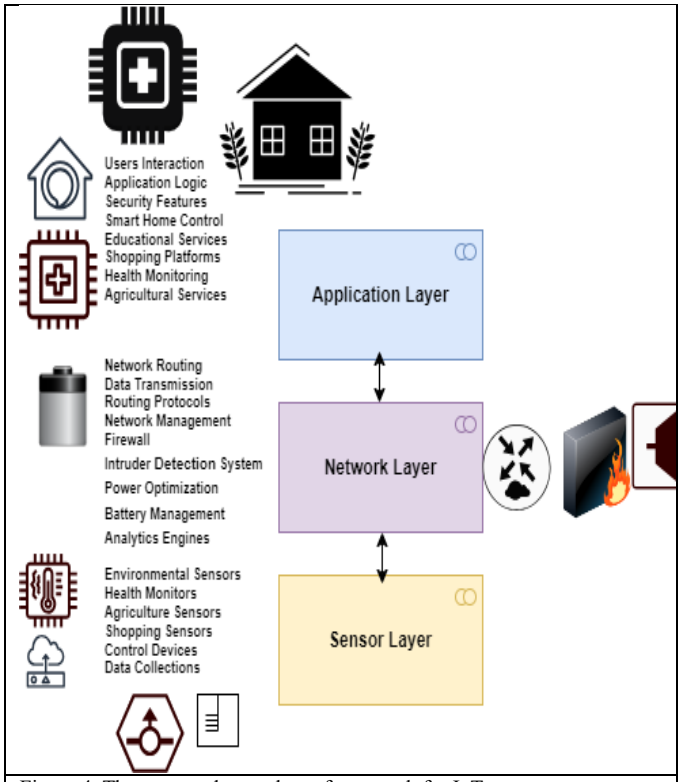

Figure 4. The proposed cross-layer framework for IoT

Application Layer: The application layer in IoT systems facilitates user interaction with web and mobile applications. This layer handles user requests and forwards them to lower layers, connecting directly to end users. It encompasses user interfaces, data processing, and application-specific functionalities. Security mechanisms at this layer ensure user authentication, access control, encryption, and secure data handling, guarding against unauthorized access and reducing risks. Additionally, the application layer supports energy-efficient data processing and application-specific energy management, using techniques like data aggregation and adaptive algorithms.

The application layer plays a crucial role in processing and analyzing sensor data, including aggregation, filtering, and analytics to extract insights. It provides a user-friendly interface for interacting with the IoT system, allowing users like healthcare professionals and agricultural experts to access data, configure settings, and receive alerts. Application layer security safeguards sensitive data and restricts access to authorized users. It defines the core logic of IoT applications, such as patient monitoring in healthcare or crop management in agriculture.

Network Layer: The physical and logical elements of a network that enable communication between systems and devices are referred to as the network layer. This includes switches, routers, firewalls, and other network equipment that manages the data flow between various network components. Network security measures in cybersecurity are made to guard against unauthorized access, data theft, and other online dangers. Operations such as routing, addressing, and data transmission take place over an IoT network. Secure routing protocols, firewalls, and intrusion detection systems, among other security measures, are implemented at this layer to help stop unauthorized network access, data tampering, and denial-of-service attacks. Data transmission integrity and confidentiality are guaranteed by protecting the network layer. Energy efficiency methods like energy-aware routing, network optimization algorithms, and traffic management can be used to achieve energy efficiency at the network layer. These actions are intended to minimize pointless data transmission, lessen network traffic, and maximize the use of network resources, all of which will ultimately result in energy savings.

The network layer establishes and manages connections between IoT devices, gateways, and the cloud or central server. It ensures reliable data transmission. This layer is responsible for routing data packets efficiently through the network. It chooses the best path for data to reach its destination while conserving energy. Network layer protocols, such as Low Power Wide Area Networks (LPWAN) or Zigbee, optimize energy consumption by allowing devices to sleep when not in use and wake up only when necessary. QoS mechanisms ensure that critical data, such as emergency alerts in healthcare or irrigation commands in agriculture, receive priority treatment.

System optimization issues involve finding trade-offs between security and energy efficiency. By examining various configurations and settings across layers, a cross-layer testing strategy assists in fine-tuning the system. It hypothesizes that a multi-layer approach involving the application, network, and sensor layers is necessary for a secure and energy-efficient architecture. This approach provides a comprehensive view of the IoT system, uncovers potential flaws and dependencies, and discovers cross-layer interactions that could result in security risks or energy inefficiency.

Sensor Layer: Refers to a group of sensors and other gadgets that are used to collect data and keep an eye out for security threats in both physical and virtual environments. Cameras, microphones, motion detectors, and other tools that can identify and store information about potential security incidents are examples of sensors. The IoT system's physical infrastructure and hardware are included in the sensor layer. To ensure security at this layer, IoT devices must be secured, tamper-resistant mechanisms must be put in place, and physical attacks like device tampering or unauthorized access to physical interfaces must be avoided. To stop physical intrusions and maintain system security overall, the physical layer must be secured. Energy-Efficient device design, energy-efficient communication protocols, and power management techniques are all ways that the sensor layer can help with energy efficiency. Examples include optimizing the power consumption of physical components and using energy-efficient wireless transmission protocols to reduce energy consumption and extend battery life.

Researching on each of the three layers (application, network, and sensor) independently is crucial for a comprehensive understanding of the IoT system (Fig. 4). It helps to identify the layer-specific vulnerabilities and weaknesses that might not be noticeable when focusing on just one layer. Additionally, it

enables the identification of trade-offs and synergies between security and energy efficiency, leading to targeted mitigation strategies and an optimal balance between the two. In conclusion, a layered architecture is vital for addressing the challenges of security and energy efficiency in IoT systems. A cross-layer approach, involving thorough examination of each layer, helps optimize IoT systems and ensures their resilience against cyber threats while balancing energy efficiency and security. The proposed architecture introduces a distinctive combination of a novel energy-efficient IoT protocol and an advanced secure architecture, setting it apart from existing literature. This dual emphasis on optimizing resources and enhancing security offers an innovative solution for more sustainable and secure IoT deployments. The summary of findings are discussed next.

IV. Results and Discussion

The test performed using application layer initially and describes the creation of an architecture to efficiently handle user requests for resources related to technological advancement. Network Layer, and Sensing Layer. Table1 lists parameters used in the system simulation. We initially tested the application layer of the architecture, which is intended to improve energy efficiency and expedite the processing of user requests while researching vulnerabilities. The power consumption before and after applying TLS analysed in Figs. 5 and 6 using the COAP browser and Wireshark.

Table 1. Parameters used in simulation

Parameters	Value
Operating System	Contiki 2.7
Routing Protocol	RPL, LOADng
Mote Type	Tmote Sky
No of Motes	3-30
Tx Ratio	100%
Rx Ratio	80%
Simulation Time	10 Minutes

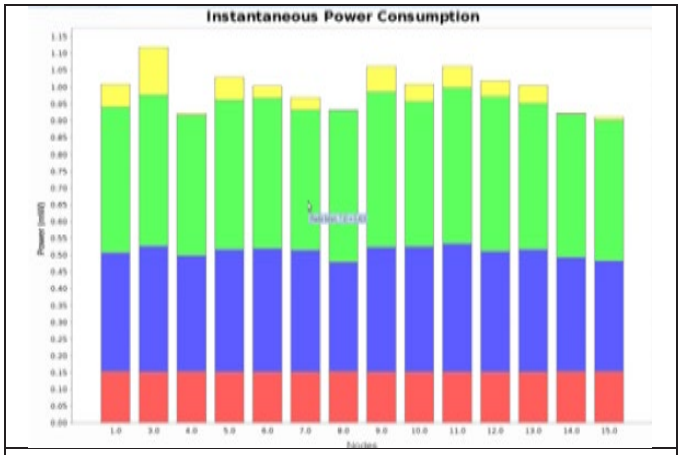

Figure 5. Power consumption before applying TLS Security

The research aims to develop a cross-layer framework for IoT communication, incorporating COAP and TLS protocols to enhance energy efficiency and security. The Wireshark filtering analysis (MQTT) is shown in Fig. 7. One can observe that the

Figure 6. Power consumption with TLS Security

communication between client and server machines is captured. Testing client-server communication using the Bevywise MQTT Broker simulator for vulnerabilities in the network layer involves thorough analysis of MQTT traffic. The study uses simulation to evaluate the framework's performance in various conditions and provide recommendations for IoT practitioners. Additionally, the study explores the use of Bevywise Simulator for network layer vulnerability testing. The simulator is configured with MQTT Broker and virtual IoT devices to monitor MQTT traffic, assess security measures, and identify vulnerabilities. The implementation of TLS (Transport Layer Security) for secure communication is demonstrated in Fig. 8.

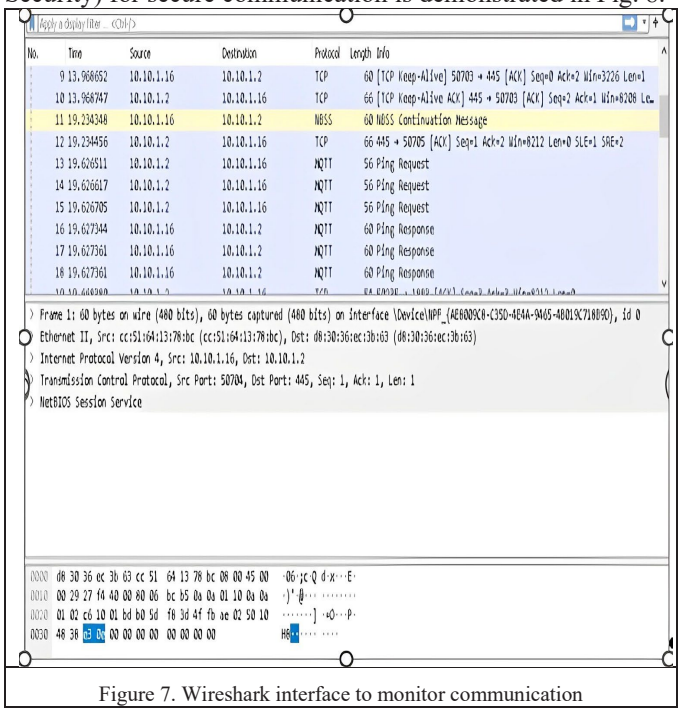

Figure 7. Wireshark interface to monitor communication

We also looked at the use of MQTT and TLS for secure communication and encrypted MQTT transmission. It

emphasizes the importance of secure communication in IoT and the need to address vulnerabilities and threats. The research seeks to optimize energy efficiency while ensuring security, contributing to the development of secure and efficient IoT systems. We observe that the data transmission is in encrypted format. When two devices are directly communicating, TLS enables transport layer encryption.

```
# WS_PORT_NO - port to start the MQTT in Websocket

# TLS_ENABLED - If set us TRUE, the product will run with SSL and WSS.
# TLS_PORT - The port at which the SSL version need to run.
# WSS_PORT_NO - port to start the MQTT SSL version in Websocket

# PREFIX - Generate the random clientid with given prefix

##########################MQTT BROKER CONFIG#############################
[CONFIG]

PORT_NO = 1883
WS_PORT_NO = 10443

TLS_ENABLED = TRUE
# TLS_PORT must be 88xx.
TLS_PORT_NO = 8883
WSS_PORT_NO = 11443

##########################Authentication Details#########################
[AUTHENTICATION]

AUTHENTICATION_ENABLED = NO
# YES || NO


##################### UserInterface Details ##########################
[UI]
UI_Http_Port = 8080

LIST_API_CLIENTS = FALSE


############# prefix for Random Clientid Generation ##################
[MQTT]

CLIENTID_PREFIX = Bevywise-
```

Figure 8. TLS enables transport layer encryption

Overall, the research focuses on improving the resilience and security of IoT systems by addressing vulnerabilities, enhancing energy efficiency, and ensuring secure communication through cross-layer frameworks and protocols. Moreover, the research could uncover ways to optimize energy efficiency while maintaining security, a critical balance in resource constrained IoT environments. Overall, the outcomes of this endeavor can contribute significantly to the development of secure and efficient IoT systems, bolstering their resilience against cyberattacks and vulnerabilities, thereby enhancing the trustworthiness of IoT deployments.

V. CONCLUSIONS

In this paper, we proposed a secure and energy-efficient cross-layer design framework for IoT applications. The framework is designed by combinig physical (sensor), network, and application layers. It offers IoT device security entails a multifaceted approach, encompassing access control, identity verification, data encryption, and intrusion detection. The protection of privacy, especially when handling personal data, is paramount. Energy conservation is vital due to resource constraints and it can be achieved through low-power communication technologies like NB-IoT, LoRaWAN, and Zigbee as well as power management and routing optimization. Delegating device tasks to edge and fog computing further reduces energy usage. IoT necessitates specific security and energy-saving measures, underscoring the need for further research. Developing a secure cross-layer framework for energy efficiency is not only a technological imperative but also a moral one to ensure safe and environmentally responsible progress in our increasingly connected and energy-efficient future. Collaboration and coordinated research efforts are indispensable in paving the way forward. An in-depth performance modelling and evaluation of the proposed cross-layer framework is suggested as an extension of the study reported here.To improve the suggested IoT architecture, future work will focus on protocol optimization, scalability assessment, real-world testing, user experience evaluation, environmental impact analysis, new tech integration exploration, and industry collaboration.

REFERENCES

[1] A. Ghasempour, “Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges,” *Inventions*, vol. 4, no. 1, 2019, doi: 10.3390/inventions4010022.

[2] M. R. Prabha and S. Sankaran, “An experimental platform for security of cyber physical systems,” *Proc. - 2019 IEEE Int. Symp. Smart Electron. Syst. iSES 2019*, pp. 123–128, 2019, doi: 10.1109/iSES47678.2019.00036.

[3] W. Yaici, K. Krishnamurthy, E. Entchev, and M. Longo, “Survey of Internet of Things (IoT) Infrastructures for Building Energy Systems,” *GIoTS 2020 - Glob. Internet Things Summit, Proc.*, 2020, doi: 10.1109/GIOTS49054.2020.9119669.

[4] E. M. Ghourab, M. Azab, and N. Ezzeldin, “Blockchain-Guided Dynamic Best-Relay Selection for Trustworthy Vehicular Communication,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 13678–13693, 2022, doi: 10.1109/TITS.2021.3126566.

[5] A. Tandon and P. Srivastava, “Location based secure energy efficient cross layer routing protocols for IOT enabling technologies,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 7, pp. 368–374, 2019.

[6] Z. Magubane, P. Tarwireyi, and M. O. Adigun, “Evaluating the Energy Efficiency of IoT Routing Protocols,” *Proc. - 2019 Int. Multidiscip. Inf. Technol. Eng. Conf. IMITEC 2019*, 2019, doi: 10.1109/IMITEC45504.2019.9015904.

[7] W. Lardier, Q. Varo, and J. Yan, “Dynamic Reduced-Round Cryptography for Energy-Efficient Wireless Communication of Smart IoT Devices,” *IEEE Int. Conf. Commun.*, vol. 2020-June, no. Section III, 2020, doi: 10.1109/ICC40277.2020.9149305.

[8] G. Callebaut, G. Ottoy, and L. Van Der Perre, “Cross-Layer Framework and Optimization for Efficient Use of the Energy Budget of IoT Nodes,” *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2019-April, 2019, doi: 10.1109/WCNC.2019.8885739.

[9] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, 2020, doi: 10.1109/JIOT.2020.2997651.

[10] D. Debnath, S. K. Chettri, and A. K. Dutta, “Security and Privacy Issues in Internet of Things,” *Lect. Notes Networks Syst.*, vol. 314, pp. 65–74, 2022, doi: 10.1007/978-981-16-5655-2_7.