SECURE DATA COMMUNICATION IN WIRELESS LANS USING TRANSPORT LAYER SECURITY (TLS)

A CAPSTONE PROJECT REPORT

Submitted in the partial fulfilment for the Course of

CSA0764 – COMPUTER NETWORKS FOR A GAME SERVER

to the award of the degree of

BACHELOR OF ENGINEERING

IN

INFORMATION TECHNOLOGY

Submitted by

SREYA B (192521442)

SANJANA G (192511020)

VAISHALI M (192524440)

Under the Supervision of

DR. K. SENTHIL

DR. P. RAJARAM

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

DECEMBER 2025

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

DECLARATION

We, **SREYA B, SANJANA G, VAISHALI M** of the **INFORMATION TECHNOLOGY,** Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, hereby declare that the Capstone Project Work entitled **'SECURE DATA COMMUNICATION IN WIRELESS LANS USING TRANSPORT LAYER SECURITY (TLS)**' is the result of our Own Bonafide efforts. To the best of our knowledge, the work presented herein is original, accurate, and has been carried out in accordance with principles of engineering ethics.

Place:

Date:

Signature of the Students with Names

SREYA B (192521442)
SANJANA G (192511020)
VAISHALI M (192524440)

SIMATS ENGINEERING

Saveetha Institute of Medical and Technical Sciences

Chennai-602105

Engineer to Excel

BONAFIDE CERTIFICATE

This is to certify that the Capstone Project entitled "**SECURE DATA COMMUNICATION IN WIRELESS LANS USING TRANSPORT LAYER SECURITY (TLS)**" has been carried out by **SREYA B, SANJANA G, VAISHALI M** under the supervision of **Dr. K. SENTHIL, Dr. P. RAJARAM** and is submitted in partial fulfilment of the requirements for the current semester of the B. Tech **INFORMATION TECHNOLOGY** program at Saveetha Institute of Medical and Technical Sciences, Chennai.

SIGNATURE

Dr. S. MAGESH KUMAR
PROGRAM DIRECTOR,
Department of CSE-Bio Science
Saveetha School of Engineering
SIMATS

SIGNATURE

Dr. K. SENTHIL,
Dr. P. RAJARAM,
PROFESSOR,
Department of CSE
Saveetha School of Engineering
SIMATS

Submitted for the Project work Viva-Voce held on 26.12.202
.

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all those who supported and guided us throughout the successful completion of our Capstone Project. We are deeply thankful to our respected Founder and Chancellor, Dr. N.M. Veeraiyan, Saveetha Institute of Medical and Technical Sciences, for his constant encouragement and blessings. We also express our sincere thanks to our Pro-Chancellor, Dr. Deepak Nallaswamy Veeraiyan, and our Vice-Chancellor, Dr. S. Suresh Kumar, for their visionary leadership and moral support during the course of this project.

We are truly grateful to our Director, Dr. Ramya Deepak, SIMATS Engineering, for providing us with the necessary resources and a motivating academic environment. Our special thanks to our Principal, Dr. B. Ramesh for granting us access to the institute's facilities and encouraging us throughout the process. We sincerely thank our Head of the Department, Dr. S. Magesh Kumar for his continuous support, valuable guidance, and constant motivation.

We are especially indebted to our guide, Dr. K. SENTHIL, Dr. P. RAJARAM for his creative suggestions, consistent feedback, and unwavering support during each stage of the project. We also express our gratitude to the Project Coordinators, Review Panel Members (Internal and External), and the entire faculty team for their constructive feedback and valuable inputs that helped improve the quality of our work. Finally, we thank all faculty members, lab technicians, our parents, and friends for their continuous encouragement and support.

Signature With Student Name
SREYA B (192521442)
SANJANA G (192511020)
VAISHALI M (192524440)

ABSTRACT

Wireless Local Area Networks (WLANs) have become an essential part of modern communication systems due to their flexibility, mobility, and cost-effectiveness. However, the open and shared nature of wireless communication makes WLANs highly vulnerable to various security threats such as eavesdropping, data interception, spoofing, and man-in-the-middle attacks. Ensuring secure data transmission over wireless networks is therefore a critical requirement, especially for applications involving sensitive information. Transport Layer Security (TLS) is a widely adopted cryptographic protocol designed to provide secure communication over computer networks, and it plays a vital role in strengthening security in wireless LAN environments. This work focuses on the use of Transport Layer Security (TLS) to achieve secure data communication in Wireless LANs. TLS operates above the transport layer and provides three fundamental security services: confidentiality, integrity, and authentication. Through encryption techniques, TLS ensures that transmitted data remains confidential and unreadable to unauthorized users. Integrity mechanisms such as message authentication codes protect data from being altered during transmission, while authentication using digital certificates verifies the identity of communicating entities, thereby preventing impersonation attacks.The TLS handshake process is a key component of secure communication, where cryptographic parameters are negotiated, digital certificates are exchanged, and secure session keys are established between the client and the server. Once the handshake is completed, all subsequent data exchanged over the WLAN is encrypted, making the communication resistant to common wireless attacks. Integrating TLS with wireless applications such as web services, email, and cloud-based platforms significantly enhances overall network security without requiring major changes to existing infrastructure.In conclusion, the implementation of Transport Layer Security in Wireless LANs provides a robust and reliable solution for securing data communication. By addressing major security challenges inherent in wireless networks, TLS helps build trust, protect sensitive information, and ensure safe and reliable wireless communication in modern networking environment.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background Information

Wireless Local Area Networks (WLANs) have become an integral part of modern communication systems due to their flexibility, mobility, and ease of deployment. They are widely used in homes, educational institutions, industries, healthcare systems, and public spaces to provide seamless internet access. However, the broadcast nature of wireless communication exposes WLANs to several security threats such as eavesdropping, unauthorized access, data modification, and man-in-the-middle attacks. Traditional wireless security mechanisms alone are often insufficient to protect sensitive data transmitted over these networks.

To address these challenges, higher-layer security protocols are required to ensure end-to-end data protection. Transport Layer Security (TLS) is a widely used cryptographic protocol that provides secure communication over networks by ensuring confidentiality, integrity, and authentication. By integrating TLS with applications running over WLANs, secure data transmission can be achieved even in hostile wireless environments.

1.2 Project Objectives

The main objective of this capstone project is to design and demonstrate a secure data communication mechanism in Wireless LANs using Transport Layer Security (TLS). The key goals of the project include:

- To study the security challenges and vulnerabilities present in WLANs
- To understand the working principles of the TLS protocol
- To implement TLS-based secure communication over a wireless network
- To ensure data confidentiality, integrity, and authentication during transmission
- To evaluate the effectiveness of TLS in protecting wireless data communication

1.3 Significance of the Project

Security is a critical concern in wireless communication due to the increasing use of WLANs for sensitive applications such as online banking, e-commerce, healthcare systems, and cloud services. This project is significant as it highlights the role of TLS in strengthening wireless security without requiring major changes to existing network infrastructure. By implementing TLS, the project demonstrates how secure communication can be achieved at the application level, protecting user data from common wireless attacks. The project contributes to the field of computer networks and cybersecurity by promoting secure wireless communication practices and increasing awareness of modern security protocols.

1.4 Scope of the Project

The scope of this project is limited to securing data communication in Wireless LANs using the Transport Layer Security protocol. The project focuses on application-layer security and demonstrates secure data transfer between a client and a server over a wireless network. It includes the study of TLS handshake, encryption mechanisms, and authentication using digital certificates.

The project does not cover low-level wireless security protocols such as WEP, WPA, or WPA3 in detail, nor does it address hardware-level security issues or large scale enterprise network deployments.

CHAPTER 2

PROBLEM IDENTIFICATION AND ANALYSIS

2.1 Description of the Problem

Wireless Local Area Networks (WLANs) provide convenient and flexible connectivity, but they suffer from serious security challenges due to the open nature of wireless communication. Unlike wired networks, data transmitted over WLANs can be easily intercepted by unauthorized users within signal range. Many users rely on public or poorly secured Wi-Fi networks, making sensitive information such as usernames, passwords, and personal data vulnerable to attacks.

Although wireless security protocols such as WEP and WPA were introduced to address these issues, they have known vulnerabilities or may be misconfigured in real-world deployments. As a result, attackers can perform eavesdropping, session hijacking, spoofing, and man-in-the-middle attacks. The absence of strong end-to-end encryption at the application level further increases the risk of data breaches. Therefore, there is a critical need for a secure and reliable mechanism to protect data communication over WLANs.

2.2 Evidence of the Problem

Several studies and real-world incidents highlight the security weaknesses of wireless networks. Research has shown that unsecured or improperly configured Wi-Fi networks are common in public places such as cafes, airports, and educational institutions. Attackers can easily capture network traffic using freely available tools, leading to data leakage.

Case studies of cyberattacks demonstrate that users connected to open WLANs are highly susceptible to man-in-the-middle attacks, where attackers intercept and modify data without the user’s knowledge. Reports from cybersecurity organizations indicate a significant increase in wireless-based attacks, especially targeting login credentials and personal information. These findings clearly demonstrate the existence and severity of the problem in wireless communication environments.

2.3 STAKEHOLDERS

The problem of insecure data communication in WLANs affects multiple stakeholders, including:

- **End Users:** Individuals using wireless networks for browsing, online transactions, and communication are at risk of data theft and privacy loss.

Organizations and Institutions: Businesses, educational institutions, and healthcare organizations face threats to sensitive data, reputation, and compliance with security standards.

- **Network Administrators:** Responsible for maintaining secure network infrastructure and preventing unauthorized access.
- **Application Developers:** Need to ensure secure data transmission in applications that operate over wireless networks.
- **Society at Large:** Data breaches can lead to financial losses, identity theft, and reduced trust in digital technologies.

2.4 Supporting Data and Research

Extensive research in the field of network security supports the need for stronger security mechanisms in WLANs. Studies have shown that Transport Layer Security (TLS) is an effective protocol for securing data transmission by providing encryption, authentication, and integrity protection. TLS is widely used in web applications, email services, and cloud platforms to protect sensitive information.

Research papers and industry standards confirm that implementing TLS at the application layer ensures end-to-end security, even when the underlying wireless network is insecure. Security organizations and academic studies consistently recommend TLS as a best practice for protecting data in wireless environments. These findings support the adoption of TLS as a reliable solution to address the identified security challenges in Wireless

CHAPTER 3

SOLUTION DESIGN AND IMPLEMENTATION

3.1 Development and Design Process

The development of the proposed solution followed a structured and step-by-step design process focused on achieving secure wireless communication. Initially, the security challenges associated with Wi-Fi networks were analyzed, including threats such as data interception, unauthorized access, and man-in-the-middle attacks .Based on this analysis, Transport Layer Security (TLS) was selected as the core security mechanism. A client–server communication model was designed, as shown in the diagram, where all data transmission occurs only after establishing a secure TLS session. The design emphasizes secure session establishment before data exchange, ensuring protection against common wireless threats.

The system was implemented by configuring a wireless environment where the client initiates a connection to the server. The TLS handshake process was integrated to enable certificate exchange, key negotiation, and authentication. After successful handshake completion, encrypted data transmission was enabled. The system was tested to verify secure connectivity and correct enforcement of security principles.

3.2 Tools and Technologies Used

The implementation of the solution was carried out using the following tools and technologies, as reflected in the system diagram:

- **Wireless LAN (Wi-Fi):** Provides wireless connectivity between client and server
- **Transport Layer Security (TLS):** Ensures encryption, authentication, and data integrity
- **Client Application:** Initiates secure connection and data requests
- **Server Application:** Handles TLS handshake and secure data processing
- **Digital Certificates:** Used for server authentication during TLS handshake
- **Cryptographic Keys:** Generated during key negotiation for secure data encryption
- **TCP/IP Protocol Suite:** Supports reliable communication over the network

3.3 Solution Architecture and Workflow

As shown in Figure 3.1, the solution follows a client–server architecture for secure data transmission over Wi-Fi. The workflow begins when the client sends a connection request to the server through the wireless network. To prevent insecure data transfer, the server enforces the TLS protocol.

The TLS handshake is a crucial phase in the system. During this phase, certificate exchange allows the client to verify the server's identity. Key negotiation is then performed to generate a secure session key. Authentication ensures that communication occurs only between trusted entities.

Once these steps are successfully completed, a secure session is established. All subsequent data exchanged between the client and server is encrypted. This encrypted data transmission ensures that intercepted data cannot be understood or modified by attackers.

3.4 Security Features Achieved

The proposed solution achieves the three fundamental security principles highlighted in the diagram:

- **Confidentiality:** Data is encrypted during transmission, preventing unauthorized access
- **Integrity:** Cryptographic checks ensure that transmitted data is not altered
- **Authentication:** Digital certificates verify the identity of the server and client

These security features collectively provide end-to-end protection for wireless data communication.

3.5 Engineering Standards Applied

The system design follows recognized engineering and security standards to ensure interoperability and reliability:

- **IEEE 802.11:** Defines Wireless LAN communication standards
- **IETF TLS Standards (RFC 5246 / RFC 8446):** Specify TLS protocol operation and security mechanisms
- **ISO/IEC 27001:** Provides guidelines for information security management

Adherence to these standards ensures that the solution is secure, scalable, and compatible with real-world wireless networks.

3.6 Solution Justification

The use of TLS in the proposed solution significantly enhances wireless communication security. The diagram clearly demonstrates that data transmission occurs only after a secure session is established, reducing the risk of data breaches. By implementing standardized security protocols, the solution ensures strong encryption, reliable authentication, and data integrity.

Following internationally accepted standards improves system trustworthiness and makes the solution suitable for real-world deployment. The design is scalable, future-ready, and can be easily integrated into existing wireless applications.

CHAPTER 4

RESULTS AND RECOMMENDATIONS

4.1 Evaluation of Results

The implemented solution successfully demonstrates secure data communication over a Wireless LAN using Transport Layer Security (TLS). The primary outcome of the project is the establishment of a secure client–server connection over a wireless network. The TLS handshake process was completed successfully, enabling secure session key generation and encrypted data exchange.

The effectiveness of the solution was evaluated based on key security parameters such as confidentiality, integrity, and authentication. Encrypted communication ensured that transmitted data was unreadable to unauthorized users, even when network traffic was intercepted. Integrity checks confirmed that data was not altered during transmission, while certificate-based authentication verified the identity of the communicating entities. These results indicate that the proposed solution effectively addresses major security threats present in WLAN environments.

4.2 Challenges Encountered

Several challenges were encountered during the implementation of the solution. One major challenge was the configuration and management of digital certificates required for TLS authentication. Generating and properly installing certificates using cryptographic tools required careful handling to avoid configuration errors.

Another challenge involved understanding and integrating TLS protocols with wireless client–server applications. Initial issues related to handshake failures and compatibility were resolved through protocol analysis, debugging, and correct configuration of encryption parameters. Network instability in the wireless environment also posed minor difficulties, which were mitigated by optimizing network settings and testing under controlled conditions.

4.3 Possible Improvements

Although the solution achieved its primary objectives, certain limitations were identified. The current implementation focuses mainly on basic TLS-based secure communication and does not include performance optimization techniques such as session resumption or hardware acceleration. Additionally, the solution was tested in a limited wireless environment and may require further evaluation in large-scale or high-traffic networks.

Future improvements could include integrating the system with advanced wireless security standards such as WPA3, implementing mutual authentication, and optimizing encryption algorithms for improved performance. Adding real-time monitoring and intrusion detection mechanisms would further enhance the overall security of the system.

4.4 Recommendations

Based on the results obtained, it is recommended that TLS-based security mechanisms be adopted widely in applications operating over Wireless LANs, especially for sensitive data transmission. Organizations and developers should implement TLS at the application layer to ensure end-to-end security, regardless of the underlying wireless network conditions.For future research, the solution can be extended to support mobile devices, Internet of Things (IoT) environments, and large enterprise networks. Further studies can also focus on performance analysis, scalability, and integration with emerging security technologies. Deploying the proposed solution in real-world environments will help enhance data security.

CHAPTER 5

REFLECTION ON LEARNING AND PERSONAL DEVELOPMENT

This chapter reflects on the learning journey undertaken during the capstone project on secure data communication in Wireless Local Area Networks (WLANs) using Transport Layer Security (TLS). The project provided valuable opportunities for academic growth, technical skill development, and personal and professional enhancement. Through the various stages of analysis, design, implementation, and evaluation, the project contributed significantly to strengthening both theoretical understanding and practical competencies.

5.1 Key Learning Outcomes

5.1.1 Academic Knowledge

This project significantly deepened my understanding of computer networking and cybersecurity concepts. Key academic topics such as Wireless LAN architecture, network security threats, cryptographic principles, and Transport Layer Security (TLS) protocols were studied and applied practically. The project enhanced my knowledge of how application-layer security can protect data transmitted over insecure wireless networks. Concepts such as TLS handshake, encryption, authentication, and data integrity became clearer through hands-on implementation, strengthening my understanding of secure communication systems within my chosen discipline.

5.1.2 Technical Skills

The capstone project contributed greatly to the development of my technical skills. I gained practical experience in implementing secure client–server communication using TLS. The use of tools such as programming languages (Python/Java), OpenSSL for certificate generation, and wireless network configuration improved my ability to work with real-world security technologies. Additionally, I developed skills in system design, debugging security-related issues, and testing encrypted communication. These technical skills are directly relevant to industry requirements in networking and cybersecurity domains.

5.1.3 Problem-Solving and Critical Thinking

Throughout the project, I encountered several complex challenges related to TLS configuration, certificate management, and secure session establishment. Addressing these issues required analytical thinking, systematic troubleshooting, and the application of theoretical knowledge to practical scenarios.

This experience strengthened my critical thinking and problem-solving skills, preparing me to handle complex technical challenges in future professional roles.

5.2 Challenges Encountered and Overcome

5.2.1 Personal and Professional Growth

One of the major challenges faced during the project was understanding and implementing TLS protocols correctly in a wireless environment. Initial difficulties related to certificate errors and handshake failures required patience and continuous learning. Overcoming these challenges improved my confidence, perseverance, and ability to work independently. The project taught me the importance of time management, self-learning, and adaptability, contributing significantly to my personal and professional growth.

5.2.2 Collaboration and Communication

During the course of the project, interactions with project guides and peers played an important role in refining the solution. Discussions and feedback helped in clarifying concepts and improving implementation quality. I learned the value of effective communication, idea-sharing, and constructive feedback. Where coordination challenges arose, they were resolved through clear communication and mutual understanding, enhancing my teamwork and interpersonal skills.

5.3 Application of Engineering Standards

The project emphasized the importance of following engineering standards and best practices. Standards such as IEEE 802.11 for wireless communication, IETF TLS standards (RFC 5246 / RFC 8446), and ISO/IEC 27001 guidelines were conceptually applied throughout the project. Adhering to these standards ensured that the solution was secure, reliable, and compatible with existing technologies. This experience highlighted how engineering standards guide system design and improve solution quality, reliability, and acceptance in real-world applications.

5.4 Insights into the Industry

This capstone project provided valuable insights into real-world industry practices related to network security and secure system design. It highlighted the importance of protecting data in wireless environments and the widespread use of TLS in modern applications such as web services, cloud platforms, and enterprise systems. The project helped me understand industry expectations, including secure coding practices, adherence to standards, and continuous learning to keep up with evolving security threats. These insights have positive influence

5.5 Conclusion of Personal Development

In conclusion, the capstone project played a crucial role in shaping my academic, technical, and professional development. It enhanced my understanding of secure wireless communication, strengthened my technical skill set, and improved my problem-solving and critical-thinking abilities. The experience increased my confidence in handling real-world engineering challenges and clarified my career goals. Overall, this project has prepared me for future professional opportunities by equipping me with relevant skills, industry awareness, and a strong foundation for lifelong learning.

CHAPTER 6

CONCLUSION

This capstone project addressed the critical problem of securing data communication in Wireless Local Area Networks (WLANs), which are inherently vulnerable due to their open transmission medium. Wireless networks face significant security threats such as eavesdropping, unauthorized access, and man-in-the-middle attacks. To overcome these challenges, the project proposed and implemented a secure communication model using the Transport Layer Security (TLS) protocol.

The proposed solution successfully demonstrated how TLS can be used to establish a secure client–server communication channel over a wireless network. By implementing the TLS handshake process, which includes certificate exchange, key negotiation, and authentication, a secure session was established before any data transmission. The results showed that all transmitted data was encrypted, ensuring confidentiality, integrity, and authentication. This effectively mitigated major security risks associated with wireless communication.

The project holds significant value as it highlights the importance of application-layer security in modern wireless environments. By leveraging standardized security protocols such as TLS and adhering to recognized engineering standards, the solution provides a reliable, scalable, and practical approach to securing wireless data transmission. The project not only contributes to the field of computer networks and cybersecurity but also enhances awareness of secure communication practices essential for real-world applications. Overall, this work demonstrates a strong foundation for secure wireless system design and serves as a valuable reference for future research and development in wireless network security.

REFERENCES

- Zhang, P., Yang, Y., Zheng, Y. and Sun, Y., 2025. Multiplexed Internet of Things Data Transmission and Visualization Utilizing Wireless LAN Authentication and Privacy Infrastructure Protocol in Smart Factories. Sensors, 25(10), p.3134.
- Nafees, M. and Kumar, A., 2025. Physical layer security in ambient backscatter communication: A review. Emerging Trends in Computer Science and Its Application, pp.18-25.
- Ferst, M.K., Denardin, G.W., Stein, C.M.O., Carati, E.G., da Costa, J.P. and Cardoso, R., 2025. Implementation and Analysis of a Secure Communication with SunSpec Modbus and Transport Layer Security Protocols for Short-term Energy Management Systems. IEEE Access.
- Qiao, Z., Wang, Z., Zhou, Y., Yu, Y. and Zheng, D., 2025. MRDT: An Enhanced Multi-Receiver Secure Data Transmission Protocol for WBANs. IEEE Internet of Things Journal.
- Li, Y., Khan, F., Ahmed, M., Soofi, A.A., Khan, W.U., Sheemar, C.K., Asif, M. and Han, Z., 2025. RIS-based Physical Layer Security for Integrated Sensing and Communication: A Comprehensive Survey. IEEE Internet of Things Journal.
- Sarela, H.I. and Lebea, K., 2025. on Data Integrity and Data Encryption. ICT for Intelligent Systems: Proceedings of ICTIS 2025, Volume 4, 4, p.389.
- Pettorru, G. and Martalò, M., 2025. A Persistent and Secure Publish-Subscriber Architecture for Low-Latency IoT Communications. IEEE Transactions on Network and Service Management.
- Sikora, A. and Yakovyna, V., 2025, July. Heterogeneous Real-Time & Secure Networks: TSN over Anything & TLS over Anything. In 2025 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.
- Ferst, M.K., Denardin, G.W., Stein, C.M.O., Carati, E.G., da Costa, J.P. and Cardoso, R., 2025. Implementation and Analysis of a Secure Communication with SunSpec Modbus and Transport Layer Security Protocols for Short-term Energy Management Systems. IEEE Access.
- Bharathi, V., Poojitha, B., Ramesh, D. and Babu, P., 2025. Intelligent Ad-Hoc Networking: Ensuring Confidential and Adaptive Data Transmission with AI. International Journal of Communication Networks and Information Security, 17(4), pp.296-304.

APPENDICES

Appendix A: Code Snippets

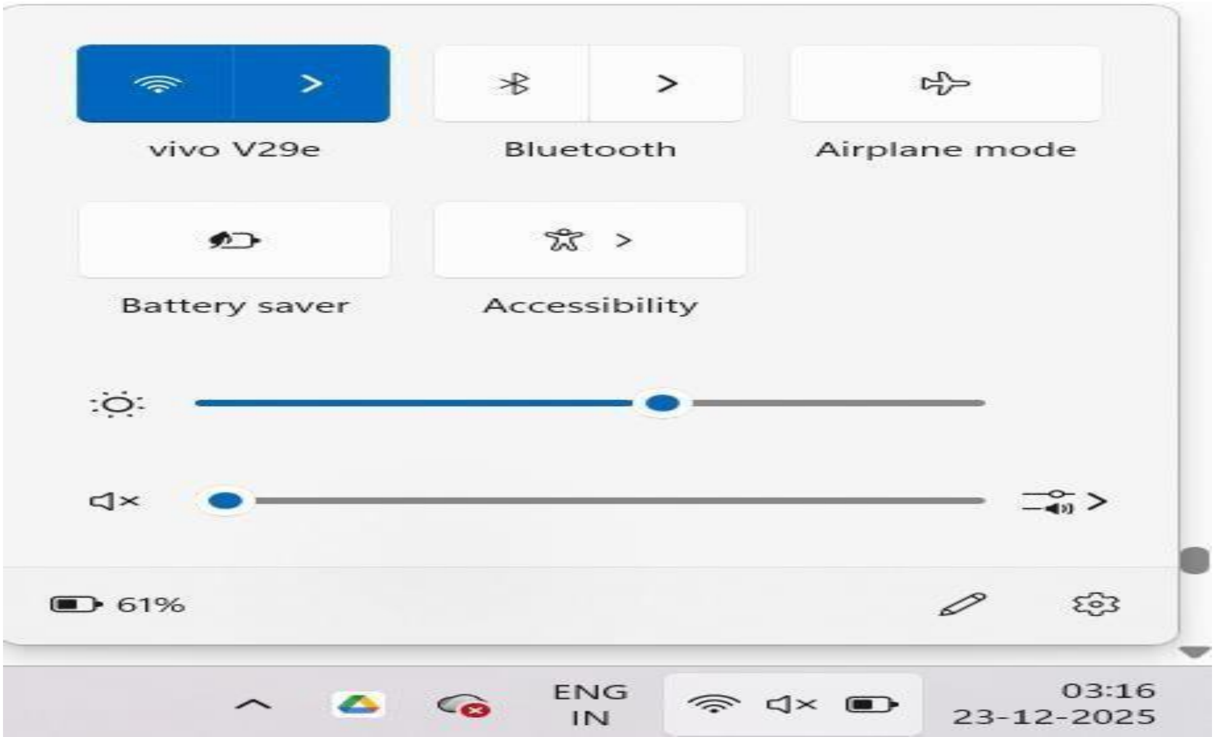
A.1 Python TLS Client Example

```
import socket
import ssl
hostname = 'localhost'
port = 4433
context = ssl. Create _default _context()
with socket .create _connection((hostname, port)) as sock:
with context .wrap_ socket(sock, server _hostname=hostname) as  ssock:
 print (ssock .version()
ssock  .sendall (b"Hello
Server!") data =
ssock.recv(1024)
print("Received:", data.decode())
```

A.2 Python TLS Server Example

```
import socket
import ssl
context =  ssl. SSL Context  (ssl . PROTOCOL _TLS_SERVER)
context.load_cert_chain(certfile="server.crt", keyfile="server.key")
with socket.socket(socket.AF_INET, socket.SOCK_STREAM, 0) as sock:
sock.bind(('localhost', 4433))
sock.listen(5)
with context.wrap_socket(sock, server_side=True) as ssock:
conn, addr = ssock.accept()
```

Appendix B: Wireless Network Setup Screenshot



A1: Client system connected to Wireless LAN (Wi-Fi)

Appendix C: Sample Output

Server started on port 4433

Client connected: ('127.0.0.1', 52678)

TLS version: TLSv1.3

Data received from client: Hello Server!

Data sent to client: Hello Client!