MANAKULA VINAYAGAR INSTITUTE OF TECHNOLOGY
PONDICHERRY UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that the mini project work entitled **"SECURE PROXY VPN WITH USER AUTHENTICATION AND ACTIVITY LOGGING"** is a bonafide work done by **J. BENNY CHRISTIAN [REGISTER NO: 22TD0316],S SITHARTH [REGISTER NO: 22TD0402] S. GURUSARAN [REGISTER NO: 22TD0331]** in partial fulfillment of the requirement for the award of B.Tech Degree in COMPUTER SCIENCE AND ENGINEERING by Pondicherry University during the academic year 2023 - 24.

PROJECT GUIDE
Mrs. P.SUGANYA, M.E,
Assistant Professor,
Department of CSE.

HEAD OF THE DEPARTMENT
Dr. S. Pariselvam, M.E, Ph.D.,
Head of the Department,
Department of CSE.

MINI PROJECT COORDINATOR
Mrs. I.Varalakshmi, M.Tech. (Ph.D),
Assistant Professor,
Department of CSE.

DECLARATION

This is to certified that the Report entitled "**SECURE PROXY VPN WITH USER AUTHENTICATION AND ACTIVITY LOGGING**" is the bonafide record of independent work done by **J. BENNY CHRISTIAN [REGISTER NO: 22TD0316],S SITHARTH [REGISTER NO: 22TD0402] S. GURUSARAN [REGISTER NO: 22TD0331]** for the award of B.Tech Degree in **COMPUTER SCIENCE AND ENGINEERING** under the supervision of **Mrs. P. SUGANYA, M.E.,** Assistant Professor Certified further that the work reported herein does not form part of any other thesis or dissertation based on which a degree or award was conferred earlier.

1. J. BENNY CHRISTIYAN
-

2. S. SITHARTH -

3. S. GURUSARAN
-

PROJECT GUIDE **HEAD OF THE DEPARTMENT**

ACKNOWLEDGEMENT

We express our deep sense of gratitude to **Theiva Thiru. N. Kesavan,** Founder, **Shri. M. Dhanasekaran,** Chairman & Managing Director**, Shri. S. V. Sugumaran,** Vice-Chairman and **Dr. K. Gowtham Narayanasamy** Secretary of **Sri ManakulaVinayagar Educational Trust, Puducherry** for providing necessary facilities to successfully complete our project and report works.

We express our sincere thanks to our beloved Principal **Dr. S. Malarkkan** for having provided necessary facilities and encouragement for successful completion of this project work.

We express our sincere thanks to **Dr.S.Pariselvam Professor and** Head **of the Department**, **Computer Science and Engineering** for his support in making necessary arrangements for the conduction of Project and also for guiding us to execute our project successfully.

We express our sincere thanks to **Mrs. P. Suganya**, **Assistant Professor**, **Computer Science and Engineering** for her/his consistent reviews which motivated us in completing the project.

We express our sincere gratitude to Mini Project coordinator **Mrs.I.Varalakshmi**, **Assistant Professor (SG)**, **Computer Science and Engineering** for her consistent reviews and suggestions which help us in effective completion of the project.

We thank all our department faculty members, non-teaching staff and my friends from Computer Science and Engineering for helping us to complete the document successfully on time.

We would like to express our eternal gratitude to our parents for the sacrifices they made for educating and preparing us for our future and their everlasting love and support. We thank the Almighty for blessing us with such wonderful people and for being with us always.

SUSTAINABLE DEVELOPMENT GOALS (SDGs) MAPPING

Title: SECURE PROXY VPN WITH USER AUTHENTICATION AND ACTIVITY LOGGING

SDG Goal : SDG Goal-11 (SUSTAINABLE CITIES AND COMMUNITIES)

SDG Goal : SDG Goal- 12 (RESPONSIBLE CONSUMPTION AND PRODUCTION)

SDG Goal -11:

In alignment with Sustainable Development Goal (SDG) 11, which seeks to make cities and human settlements inclusive, safe, resilient, and sustainable, this project contributes by enhancing secure, efficient communication and data management. By ensuring encrypted, tamper-resistant data transmission, the system supports the reliability and safety of urban digital infrastructure, which is increasingly crucial in smart cities. The secure client-server communication model, using advanced cryptographic techniques, prevents unauthorized access and data breaches, which are essential for maintaining the integrity of urban systems that rely on sensitive information. Furthermore, this project's efficient encryption and processing reduce computational overhead, enabling it to operate smoothly in resource-constrained devices often used in IoT-based smart city frameworks. This efficiency supports sustainable digital infrastructure, helping urban areas manage resources with minimal environmental impact and reinforcing the resilience of urban communication networks.Moreover, by reducing the potential for data breaches or cyberattacks, the project supports a safer urban environment for residents and authorities alike. This reliability is especially vital for smart cities, where interconnected systems require constant communication and data integrity to provide consistent, responsive services. By embedding resilience in urban data flows, this project enables cities to better withstand and adapt to disruptions, fostering a secure, sustainable urban ecosystem in line with SDG 11's objectives.

SDG Goal -12:

Sustainable Development Goal (SDG) 12, which promotes sustainable consumption and production patterns, is significantly supported by this project's approach to secure data communication in digital systems. By enhancing the precision, efficiency, and security of data management, the project helps optimize resource use, reducing waste and the environmental footprint of digital infrastructures. The secure data exchange model ensures accurate, tamper-resistant transactions, which is essential for systems managing valuable or sensitive data, allowing only verified access and reducing unauthorized interventions or resource misuse.Moreover, the project's lightweight encryption mechanisms reduce energy consumption by optimizing data handling efficiency without compromising security. This energy efficiency is particularly beneficial in IoT and smart city applications, where devices must operate on limited power or computational capacity. By supporting sustainable data management and efficient resource use, the project contributes to longer-lasting devices, less frequent maintenance needs, and minimized operational costs, aligning with sustainable production goals.The project also integrates with monitoring and compliance systems to maintain accurate records of data transactions, supporting regulatory adherence and sustainability standards. This data precision enables operators to monitor performance, identify potential inefficiencies, and proactively adjust to optimize resource allocation.

ABSTRACT

The "Secure VPN Communication System Using ECDH and AES-256-GCM" project introduces a robust solution for encrypted client-server communication. By integrating Elliptic Curve Diffie-Hellman (ECDH) for key exchange and AES-256-GCM for encryption, it establishes a secure channel, safeguarding data integrity and confidentiality across network transactions.ECDH ensures secure key exchange without directly transmitting encryption keys, generating unique session-specific keys for each connection. This approach reduces the risk of interception, offering enhanced security in key management—a critical aspect for maintaining secure communication over untrusted networks.AES-256-GCM further strengthens data protection by encrypting all HTTP/HTTPS requests sent through the VPN tunnel. The Galois/Counter Mode (GCM) not only encrypts the data but also provides authentication, ensuring that any attempts at data tampering are immediately detected, preserving data integrity.Within this secure framework, the client initiates encrypted requests, which are decrypted by the server before processing. The server then responds with encrypted data, ensuring that every data transfer is protected from unauthorized access. This encrypted tunnel allows for safe web browsing and resource access.The project serves as an educational tool, demonstrating key cryptographic principles and the practical implementation of VPN technology. By using ECDH and AES-256-GCM, it provides a real-world example of secure, efficient communication, highlighting modern cryptographic methods.In comparison to traditional VPN solutions, this project offers lower computational overhead, making it ideal for resource-constrained devices. It exemplifies how advanced cryptographic techniques can enhance data security and efficiency.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
API	Application Programming Interface
DBMS	Database Management System
DH	Diffie-Hellman (for key exchange protocol)
ECDH	Elliptic Curve Diffie-Hellman
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LAN	Local Area Network
OTP	One-Time Password
PKI	Public Key Infrastructure
SQL	Structured Query Language
TLS	Transport Layer Security
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
JWT	JSON Web Token
SSH	Secure Shell
RSA	Rivest-Shamir-Adleman (
SSL	Secure Sockets Layer
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Message Authentication Code
JSON	JavaScript Object Notation
UID	User Identifier
DNS	Domain Name System