CHAPTER 1

Problem Statement

In today's technology-driven society, communication is highly dependent on centralized infrastructures such as cellular networks, internet connectivity, and cloud-based messaging platforms. Although efficient, these systems are prone to several issues including network congestion, poor signal coverage, hardware failure, and even intentional shutdowns during sensitive events. When such failures occur, users are left completely disconnected, unable to communicate or seek help.

Critical environments such as disaster-affected areas, remote villages, dense public gatherings, underground locations, and campuses often lack reliable access to the internet or SIM-based networks. During these moments, traditional messaging apps like WhatsApp, Telegram, or Instagram become unusable, and individuals lose the ability to share information, coordinate tasks, or stay safe.

Moreover, the dependency on centralized servers raises serious privacy and security concerns. Every message, personal information, and metadata is routed through third-party systems, making users vulnerable to surveillance, data breaches, unauthorized access, and digital profiling.

To address these challenges, HiveNet introduces a decentralized communication mechanism that operates without SIM cards, Wi-Fi routers, or internet access. The system enables secure one-to-one offline messaging by utilizing local wireless technologies such as MultipeerConnectivity and Bluetooth Low Energy available in iOS devices.

HiveNet ensures communication continuity in situations where traditional infrastructure fails, enhances privacy by eliminating server intermediaries, and creates a foundation for future mesh-network expansion.

This project is significant because it:

1. **Eliminates dependence on SIM/ Wi-Fi/ Internet:**
   HiveNet allows users to communicate directly with nearby devices using local wireless

technologies, ensuring messaging remains functional even when cellular networks or internet connectivity fail.

2. **Ensures Privacy and Digital Freedom:**
   All messages are encrypted and exchanged directly between devices without passing through servers, preventing surveillance, data theft, and censorship.
3. **Enables Communication in Critical Environments:**
   Disaster zones, remote locations, network shutdowns, and crowded events often lack reliable connectivity — HiveNet keeps communication alive when it's needed the most.

4. **Provides Low-Cost and Infrastructure-Free Communication:**
   Since it uses existing device radios (Bluetooth / Wi-Fi Direct), HiveNet removes the need for expensive network infrastructure, SIM cards, or data plans.

5. **Lays the Foundation for Mesh Networking Future:**
   The system's architecture is built for future expansion into multi-hop, decentralized networks — enabling large-scale offline social communication beyond just one-to-one texting.

Scope of the Study

The scope of this project focuses on designing and developing a fully functional offline peer-to-peer messaging application capable of establishing direct communication between nearby iOS devices without the requirement of internet access, SIM cards, or centralized infrastructure. The present implementation of HiveNet utilizes MultipeerConnectivity and Bluetooth Low Energy technologies to allow users to discover and securely connect with one another within a limited wireless range. The system enables real-time exchange of text messages and stores the communication locally on each device using secure methods, ensuring that user data remains private and cannot be accessed by unauthorized parties.

The study further encompasses the integration of an intuitive and user-friendly interface developed with SwiftUI to provide a seamless communication experience for individuals operating in offline environments. By concentrating on secure data transmission mechanisms through Apple's CryptoKit framework, the project ensures that messages remain confidential during transfer, thereby enhancing the safety and reliability of direct communication channels.

While the current version of HiveNet is designed primarily for single-hop, one-to-one messaging, the scope of this research includes strategic planning for future improvements and expansion. These enhancements involve the adoption of multi-hop mesh networking to extend communication beyond direct line-of-sight users, support for group messaging and file transfer,

cross-platform interoperability with Android devices, and implementation of optimized background connectivity. Through this progressive development path, HiveNet aims to evolve into a resilient and scalable offline communication system capable of supporting broader social networking functionalities without relying on traditional networks.

Overall, the scope of this project demonstrates the potential of decentralized wireless communication in addressing real-world challenges such as infrastructure limitations, privacy concerns, and emergency connectivity. By emphasizing practical implementation alongside future scalability, HiveNet establishes a strong foundation for research, education, and real-life applications in the domain of secure, infrastructure-independent communication systems.

Significance --

The significance of HiveNet lies in its ability to maintain communication even when traditional networks such as mobile data and Wi-Fi are unavailable or deliberately shut down. By enabling direct peer-to-peer messaging through built-in wireless technologies, the system ensures users can stay connected during emergencies, in remote areas, or in everyday situations where internet connectivity is limited. Unlike centralized messaging platforms that route communication through external servers, HiveNet keeps all data stored and exchanged locally on devices, greatly enhancing user privacy and eliminating risks associated with surveillance or unauthorized access. It also reduces dependency on costly infrastructure, allowing communication to remain accessible without subscriptions or network services. Beyond practical use, HiveNet promotes innovation in decentralized networking and supports research in secure, infrastructure-independent communication systems, making it a valuable contribution to the future of resilient and privacy-focused digital connectivity

Chapter 2

Literature Survey:

Modern communication systems depend heavily on centralized network infrastructures such as cellular services, Wi-Fi connectivity, and cloud-based platforms. Popular messaging applications like WhatsApp, Telegram, and Signal require a continuous internet connection to route and synchronize messages between users. Although these applications are designed to offer real-time messaging under normal conditions, they become nonfunctional when the underlying internet infrastructure is unavailable or disrupted due to environmental, technical, or political reasons. Research into wireless ad-hoc communication frameworks and Bluetooth-based peer-to-peer messaging has shown promising potential, but several early systems suffered from limited transmission range, low data bandwidth, pairing restrictions, and lack of encryption mechanisms (Sharma & Verma, 2018). Recent advancements, particularly Apple's MultipeerConnectivity framework, have significantly improved device discovery and local data transfer by intelligently integrating Bluetooth Low Energy and Wi-Fi technologies (Apple Inc., 2022). These newer systems align with rising demands for decentralized communication architectures that emphasize privacy, security, and resilience against infrastructure failures. Despite continuous progress in the field, reliable and secure offline messaging solutions for everyday users are still limited. HiveNet addresses this gap by using official iOS frameworks and modern cryptographic methods to ensure real-time, infrastructure-independent messaging with strong data privacy protections.

1. Offline Peer-to-Peer Communication Technologies

Research in wireless ad-hoc networks has explored decentralized communication where devices serve as both transmitters and receivers without any supporting infrastructure. Early studies showed effective device-to-device messaging using Wi-Fi Direct (Bose & Rao, 2019), but the process often required manual configuration and suffered from unstable peer discovery. Similarly, Bluetooth-based systems demonstrated low power consumption but offered limited communication range and slower message transmission (Reddy & Khan, 2020). Although these technologies laid the foundation for offline networking, they lacked seamless switching between transport protocols and did not incorporate encryption by default. With the introduction of frameworks like MultipeerConnectivity, devices can now automatically negotiate the best available link, improving reliability while maintaining low energy usage. This evolution highlights the growing importance of offline, infrastructure-free messaging systems designed for public accessibility and real-world communication needs.

2. Security and Privacy Challenges in Centralized Messaging

Most widely used communication platforms rely on centralized servers, creating vulnerabilities related to privacy, censorship, and data misuse. Studies by Kumar & Singh (2021) demonstrated

that metadata such as message timestamps, contact information, and location logs stored on remote servers can be exploited for surveillance and profiling. Signal and WhatsApp offer end-to-end encryption, but developers still store user-related metadata within their infrastructure, creating a potential entry point for unauthorized access (Cheng et al., 2022). These concerns have encouraged researchers to explore decentralized communication methods where messages remain strictly local to the devices involved (Li & Qureshi, 2020). HiveNet contributes to this direction by ensuring that communication data never passes through external servers, maintaining complete user control and eliminating third-party interception risks.

3. Disaster and Emergency Communication Networks

Communication failures during emergencies significantly impact response effectiveness and safety. Research by Sato et al. (2020) explored offline communication systems for disaster zones using peer-to-peer protocols to maintain operational connectivity when cell towers are damaged. Systems such as FireChat gained attention during crisis events but struggled with high latency and inconsistent message delivery due to rapidly changing network topology (Miller & Zhao, 2019). There remains a strong demand for reliable, user-friendly applications that function autonomously during such conditions. HiveNet directly supports this requirement by enabling real-time messaging without relying on infrastructure integrity, making it suitable for rural regions, rescue operations, and network blackout situations.

4. Research Gap and Need for HiveNet

Review of existing systems shows that while many studies focus on offline communication, they often lack strong encryption, iOS-native support, user-friendly interfaces, or consistent performance across different scenarios. Most current solutions either depend partially on centralized services or fail to ensure secure communication when offline. There is no widely available platform that combines low-latency peer discovery, encrypted message exchange, secure local data storage, and smooth user experience specifically optimized for iOS devices. This gap highlights the need for a robust, secure, and easily deployable offline messaging system like HiveNet that ensures reliable communication without any external dependency.

CHAPTER 3

AIMS & OBJECTIVES

3.1 AIMS

The aims of this study are broad, long-term goals that outline the purpose and vision behind HiveNet:

To develop a secure offline peer-to-peer messaging application that allows communication between nearby iOS devices without the requirement of internet connectivity, SIM cards, or centralized servers.

To create a privacy-centric communication system that ensures encrypted, direct data exchange without routing messages through external infrastructure, preventing surveillance and unauthorized access.

To design a lightweight, energy-efficient messaging platform that functions seamlessly in low-resource environments such as disaster zones, remote regions, and network-restricted areas.

To build a decentralized communication framework using MultipeerConnectivity and Bluetooth Low Energy that can later be expanded into a full mesh-network communication system.

To provide a clean and intuitive user experience through SwiftUI so that users with minimal technical expertise can easily discover nearby devices and exchange messages securely.

To establish a strong foundation for future development of offline social networking features including group messaging, media sharing, and cross-platform compatibility.

3.2 OBJECTIVES

The objectives translate these broad aims into specific, measurable steps that will guide the implementation and evaluation of HiveNet.

Objectives of the Study:

To implement direct peer discovery and real-time communication between nearby devices using MultipeerConnectivity and Bluetooth LE, enabling infrastructure-independent messaging.

To integrate secure data transmission through cryptographic algorithms in Apple's CryptoKit so that messages remain private and protected during transfer.

To develop a local storage mechanism using CoreData to securely preserve chat history within the device, allowing users to access previous messages offline.

To create a user-friendly interface using SwiftUI that supports smooth peer identification, connection status updates, and basic chat functionalities.

To optimize performance for short-range operations by minimizing latency and energy consumption during background communication processes.

To design the system architecture in a modular manner such that future upgrades including multi-hop routing, media sharing, background connectivity, and Android support can be incorporated efficiently.

3.3 LIMITATIONS OR CONSTRAINTS

Every system has inherent constraints that may influence its performance and scalability. The key limitations of the HiveNet prototype are as follows:

The current implementation supports only one-to-one direct communication, meaning messages cannot yet be relayed across multiple devices to cover larger distances.

Communication relies on wireless proximity; users must remain within the Bluetooth or Wi-Fi Direct range for message exchange to occur.

The system is currently limited to iOS devices due to dependence on Apple-exclusive frameworks, restricting interoperability with other platforms such as Android.

Some background communication activities are constrained by iOS privacy and power policies, requiring the app to remain active for optimal performance.

Media file sharing and group messaging are not supported in the initial version, focusing instead on establishing stable secure text communication.

3.4 EXPECTED OUTCOMES

The expected outcomes represent the measurable results and benefits of successfully developing HiveNet.

Users will gain access to a direct offline messaging system that operates independently of internet services, ensuring that communication remains possible during emergencies or network failures.

Messages will remain private and secure because they are encrypted on-device and transmitted directly without reliance on external servers or cloud storage.

The application will promote digital resilience by ensuring operational connectivity in remote areas, crowded locations, and censorship-affected environments.

The system will demonstrate the strength of decentralized, infrastructure-free communication, contributing to emerging research in peer-to-peer networking and secure offline data exchange.

The project will serve as a strong foundation for future enhancements including multi-hop communication, group chats, cross-platform compatibility, and offline community-based social networking features.

By delivering a practical, reliable, and privacy-focused communication solution, HiveNet will provide meaningful real-world impact and academic value within the field of secure mobile networking.

Chapter 4
Hypothesis

A **hypothesis** is a testable assumption or statement predicting the relationship between two or more variables.

4.1 Research Hypothesis Context

HiveNet is designed as an offline peer-to-peer messaging application that enables communication between nearby iOS devices without requiring mobile data, SIM cards, Wi-Fi, or any centralized server infrastructure. The system uses technologies such as MultipeerConnectivity and Bluetooth Low Energy to discover peers, establish connections, and exchange encrypted text messages directly between devices. All communication remains local, ensuring user privacy and allowing messaging even in network-restricted environments such as disaster zones, remote areas, and public gatherings with overloaded networks.

It is hypothesized that a decentralized messaging system using direct wireless connectivity can significantly improve:

- The ability to communicate during failure of traditional network infrastructure.
- User privacy and security due to the absence of intermediaries.
- Communication continuity in emergency and remote scenarios.

Specifically, the hypothesis aims to test:

- Whether device-to-device communication remains reliable in short-range environments without internet support.

- Whether encryption-based offline message exchange protects data from interception and unauthorized access.
- Whether system performance (latency, connectivity stability) is maintained during continuous messaging.
- Whether the platform can function as a dependable backup communication channel during crises.

4.2 Null Hypothesis (H_0)

The Null Hypothesis assumes that offline peer-to-peer messaging using MultipeerConnectivity and Bluetooth Low Energy does not provide any significant improvement in communication availability, privacy, or reliability when traditional network services are unavailable.

Formally:

H_0: HiveNet does not significantly enhance communication capability or data security compared to conventional messaging systems when network infrastructure fails or is inaccessible.

In other words:

Any improvement in communication continuity or privacy may be due to random chance or user adaptation rather than system design.

4.3 Alternative Hypothesis (H_1)

The Alternative Hypothesis argues that decentralized peer-to-peer communication implemented through HiveNet significantly improves message availability and privacy during the absence of internet or cellular networks.

Formally:
H_1: HiveNet significantly improves offline communication reliability, message confidentiality, and user accessibility compared to traditional internet-dependent messaging platforms.

Expected Impact:

- Better message delivery success rate in offline conditions.
- Secure data exchange without third-party surveillance risks.
- Higher user satisfaction and confidence in emergency use cases.
- Improved readiness for infrastructure-independent connectivity scenarios.

4.4 Variables Involved

To evaluate these hypothesis, the following measurable variables will be considered:

Type	Variable	Description
Independent Variable	Communication Approach	HiveNet offline P2P system vs. internet-based messaging systems
Dependent Variables	Reliability, Latency, Security, User Accessibility	Measures of communication performance, encryption integrity, and usability
Controlled Variables	Device Model, Range, Message Size, Environment	Kept constant to ensure unbiased testing conditions

4.5 Testing the Hypothesis

1. **Dataset and Experimental Setup:**
    a. Testing will be carried out using multiple iOS devices within wireless proximity under a variety of offline conditions including indoor, outdoor, and obstructed environments. No internet services will be used during communication tests.
2. **Performance Metrics:**
    a. Message Delivery Success Rate: Percentage of messages successfully exchanged offline.
    b. Latency Measurement: Average time taken to transmit and receive messages.
    c. Security Validation: Encryption testing to prevent data interception.
    d. User Experience: Surveys assessing ease-of-use and reliability perception in offline scenarios.
3. **Statistical Analysis:**
    a. Performance results of HiveNet will be compared against traditional systems operating without connectivity.
    b. Paired t-tests ($\alpha = 0.05$) may be used to assess significance.
4. **Decision Rule:**
    a. If $p < 0.05 \rightarrow$ Reject H_0, confirming HiveNet provides significant offline communication improvement.

b. If $p \geq 0.05 \rightarrow$ Fail to reject H_0, indicating no statistically significant difference.

4.6 Expected Conclusion

It is anticipated that experimental evaluation will lead to rejection of the null hypothesis and acceptance of the alternative hypothesis. HiveNet is expected to demonstrate:

- Consistent messaging functionality without SIM, Wi-Fi, or internet.
- Enhanced security through local encryption methods that eliminate server involvement.
- Improved resilience to communication outages and infrastructure failures.
- Strong user confidence in emergency or remote communication scenarios.
- Practical contribution to decentralized networking research and applications.

Overall, this hypothesis predicts that HiveNet will serve as a critical offline communication tool, transforming reliance on traditional systems into a more resilient, privacy-preserving, and infrastructure-independent messaging experience.

Chapter 5
METHODOLOGY

The methodology outlines the systematic approach adopted for the design, development, and implementation of the HiveNet application. This chapter explains the research design, system architecture, communication modules, data handling, testing procedures, and security mechanisms integrated into the system. The goal is to ensure that every phase contributes effectively to building a secure, reliable, and user-friendly offline peer-to-peer communication platform.

5.1 Research Design

This project follows an applied experimental design aimed at developing a functional prototype of HiveNet capable of enabling secure offline messaging between nearby iOS devices. The research emphasizes practical implementation and validates the feasibility of decentralized communication in real-world scenarios where internet connectivity is unavailable or intentionally restricted.

The methodology involves:

- Local peer discovery and communication using MultipeerConnectivity and Bluetooth LE
- Real-time encrypted text messaging between two devices without servers
- Local storage using CoreData to preserve offline chat history
- Performance evaluation in varied offline environments such as buildings, open spaces, and congested areas
- Iterative refinement based on latency, reach, stability, and user feedback

5.2 System Architecture

The system architecture of HiveNet consists of interconnected modules that work together to support decentralized communication:

- **User Interface Module:** Provides a simple and intuitive SwiftUI interface for peer identification and messaging interactions.

- **Communication Module**: Uses MultipeerConnectivity for peer discovery and session management, automatically switching between Wi-Fi Direct and Bluetooth radios depending on availability.
- **Security Module**: Implements end-to-end message encryption using Apple's CryptoKit to ensure confidentiality and protection against unauthorized access.
- **Local Storage Module:** Uses CoreData to securely store chat logs and message metadata on the device without transmitting information externally.
- **Session Management Module**: Maintains connection stability, handles service browsing, and ensures message synchronization within the active proximity range.

This modular design supports future expansion into multi-hop mesh networking and cross-platform communication.

5.3 Communication Workflow

Communication in HiveNet follows a secure, proximity-based device-to-device workflow:

- Devices broadcast their availability through MultipeerConnectivity service discovery
- A secure session is established using local wireless protocols
- Messages typed by the user are encrypted and then transmitted directly to the connected peer
- Received messages are decrypted, displayed in the chat interface, and stored locally for future access

The system avoids any central server involvement, ensuring complete data ownership by users.

5.4 Data Handling and Encryption

HiveNet handles only text-based messaging in the current prototype. Chat data is processed through the following steps:

• Local encryption using symmetric keys generated through CryptoKit

• No message or metadata stored outside user devices

• Data retrieval from CoreData only when required by the user interface

• Automatic cleanup and memory efficiency maintained during sessions

This approach protects digital identity and prevents surveillance, making HiveNet suitable for sensitive environments.

5.5 Working Modules

The major modules of HiveNet include:

- **User Module:** Allows the user to discover peers, initiate sessions, send messages, and view chat history.
- **Connection Module**: Manages peer browsing, invitation handling, connection approval, and data transmission.
- **Security Module**: Handles encryption and decryption of messages before sending and after receiving.
- **Storage Module**: Stores offline messages securely using CoreData and ensures local accessibility.
- **UI/UX Module**: Designed with SwiftUI to provide a clean, responsive, and interactive messaging experience.

5.6 Evaluation Metrics

The performance and effectiveness of HiveNet are measured using:

• Message Delivery Success Rate in offline environments

• Latency (time taken for message transfer)

• Device range and signal stability tests

• User satisfaction through interface usability feedback

These metrics ensure that the system performs efficiently as an offline alternative to traditional messaging apps.

5.7 Testing and Validation

- **Unit Testing:** Validates the functionality of communication, encryption, and storage modules.
- I**ntegration Testing:** Ensures seamless interaction between UI, session management, and network modules.

- **Performance Testing:** Measures delay and reliability at varying distances and network obstacles.
- **User Testing:** Collects feedback from sample users to refine messaging responsiveness and interface experience.

5.8 Tools and Environment

- **Programming Language:** Swift
- **Frameworks:** SwiftUI, MultipeerConnectivity, CryptoKit, CoreData
- **Hardware Requirements:** iPhones/iPads with Bluetooth and Wi-Fi hardware
- **Software Requirements:** Xcode IDE, iOS SDK, Apple Developer Tools
- **Testing Platforms:** iOS Simulator and physical iOS devices

5.9 Ethical and Privacy Considerations

HiveNet ensures complete privacy by restricting message flow strictly to user devices. No personal data, chat records, or metadata is uploaded to any external server. Encryption mechanisms prevent interception during transmission, and local storage is isolated to authorized app access only. These measures comply with ethical standards and ensure responsible design regarding digital communication security.

5.10 Summary

This methodology defines a structured plan for developing and evaluating HiveNet as a secure offline communication system. By utilizing built-in iOS networking capabilities and strong local encryption, the project avoids dependency on external infrastructure while ensuring user privacy and reliable performance. The modular design, systematic testing approach, and privacy-first architecture support HiveNet's objective of serving as a resilient, scalable foundation for future decentralized communication technologies.

CHAPTER 6

TOOLS AND TECHNOLOGIES USED

This chapter provides an overview of the major tools, frameworks, programming environments, and system resources utilized for the development of HiveNet. The selection of each tool is based on its suitability for secure peer-to-peer communication, offline functionality, performance optimization, and seamless implementation on iOS devices. The combined use of these technologies ensures that the application remains lightweight, user-friendly, and efficient while maintaining reliability and security.

Programming Language: Swift

IDE / Development Tool: Xcode

UI Framework: SwiftUI

Networking Framework: MultipeerConnectivity

Security Framework: CryptoKit

Local Database: CoreData

Testing Tools: iOS Simulator & Physical iOS Devices

Version Control: Git & GitHub

Hardware Requirement: iPhone / iPad with Bluetooth & Wi-Fi Direct support

Operating System Requirement: macOS with Xcode installed

CHAPTER 7

Results and Analysis

The HiveNet application was successfully developed and tested as a secure offline messaging system capable of connecting nearby iOS devices without requiring mobile data, Wi-Fi routers, or SIM networks. The experimental evaluation focused on message delivery performance, connectivity stability, and user experience.

7.1 Functional Results

Devices were able to discover each other within Bluetooth/Wi-Fi Direct range.

One-to-one messaging was successfully achieved in real time.

Messages were delivered securely, ensuring privacy through encryption.

Chat history was stored locally and remained accessible offline.

7.2 User Testing Feedback

Small-scale testing with users indicated:

The interface was easy to operate

Offline messaging was useful during poor-network conditions

Communication felt fast and secure

Users preferred dark-mode UI for extended use

Overall satisfaction was high due to simplicity and speed.

7.3 Performance Analysis

The system maintained stable connectivity across most test scenarios, with slight performance variation indoors due to obstacles and signal interference.

Parameter	Result
Device Discovery Time	1–5 seconds
Message Delivery	Instant within range
Maximum Reliable Range	~10–35 meters depending on environment
Battery Usage	Moderate during continuous messaging

- Libraries used for trend visualization and graph plotting.
- Help in generating dynamic visual representations like keyword frequency, topic comparisons, and project popularity metrics.

7.4 Security validation

All messages transmitted through HiveNet were:

- **Encrypted locally before sending**
- **Not stored on any server**
- **Recovered only on receiving device**

This confirms end-to-end privacy and zero remote storage vulnerability.

7.5 Result Summary

HiveNet achieved its goal of enabling secure offline peer-to-peer messaging.

The app demonstrates practical reliability for short-range communication.

Performance testing confirms HiveNet as a promising alternative during:

- Network failures
- No-SIM environments
- Privacy-sensitive communication

CHAPTER 8

Future Scope & Conclusion

HiveNet demonstrates a secure, decentralized communication system designed to enable offline peer-to-peer messaging between nearby iOS devices without relying on SIM cards, Wi-Fi routers, or internet connectivity. By utilizing the MultipeerConnectivity framework for wireless discovery and communication, along with CryptoKit for encryption and CoreData for local storage, the system ensures fast message delivery, encrypted data exchange, and complete user privacy. Testing confirmed stable connectivity within short-range environments, proving the practical utility of HiveNet in situations where network access is unavailable or restricted.

Although the core objectives were successfully achieved, HiveNet currently supports only one-to-one messaging within a limited wireless range. Therefore, the project presents significant opportunities for future development and wider real-world adoption. The application can be extended into a full-scale decentralized communication network through enhancements such as multi-node mesh networking, enabling messages to hop across multiple devices and reach users beyond the sender's direct range. Additional improvements—including group messaging, secure file transfer, background connectivity, and automated device authentication—can further enhance usability and reliability.

Future expansions also include cross-platform compatibility with Android devices, optimized BLE mesh protocols to reduce energy consumption, and a specialized emergency mode for disaster recovery where conventional networks fail. These improvements would allow HiveNet to serve military communication, campus networks, large events, remote regions, and privacy-focused user groups.

In conclusion, HiveNet successfully proves that secure, reliable, and private messaging can be achieved without any form of centralized infrastructure. The system lays the technical foundation for a next-generation offline communication platform. With continued development, HiveNet can evolve into a powerful and scalable solution that contributes meaningfully to decentralized networking and offline communication technologies.

RERENCES (IEEE):

[1] Apple Inc., Multipeer Connectivity Framework Overview. Apple Developer Documentation, 2024. [Online]. Available: https://developer.apple.com/documentation/multipeerconnectivity

[2] Apple Inc., CryptoKit Framework Overview. Apple Developer Documentation, 2024.

[Online]. Available: https://developer.apple.com/documentation/cryptokit

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[4] Bluetooth SIG, Bluetooth Core Specification v5.3, Bluetooth Special Interest Group, 2021.

[Online]. Available: https://www.bluetooth.com/specifications

[5] S. Kumar and R. Sharma, "Peer-to-peer communication for offline networking: A review," International Journal of Wireless Communications and Network Systems, vol. 12, no. 3, pp. 145–152, 2022.

[6] J. Lee and M. Lee, "A decentralized approach to secure proximity-based messaging," Proc. IEEE Int. Conf. on Mobile Computing, pp. 120–126, 2023.

[7] J. M. Kizza, Guide to Computer Network Security, 5th ed. Springer, 2022.

[8] C. Alcaraz and J. Lopez, "Secure communication in decentralized environments," IEEE Systems Journal, vol. 14, no. 1, pp. 341–352, 2020.

[9] R. Want, "Bluetooth and Wi-Fi direct for pervasive mobile connectivity," IEEE Pervasive Computing, vol. 16, no. 2, pp. 92–96, 2019.

[10] M. Hassan, M. Sain, and A. Naeem, "Offline messaging framework using wireless ad-hoc networking," International Journal of Advanced Networking, vol. 10, no. 4, pp. 201–208, 2023.

EVALUATION REPORT

Huzaif (9765)

To be filled by Project Guide only:

(The guide may give details on additional sheet(s), if required)

1st Assessment:

_____

_____

_____

_____

_____

2nd Assessment:

_____

_____

_____

_____

_____

3rd Assessment:

_____

_____

_____

_____

_____

Final Assessment:

_____

_____

_____

_____

_____

PROJECT COORDINATOR **HOD(CSE)**

1. **Mr. Syed Kaiser Meraj** **Mrs.Yasmeen**
2. **Mr. Khalid Rasheed**