International Journal of Interpreting Enigma Engineers (IJIEE)

https://ejournal.svgacademy.org/index.php/ijiee/

OPEN ACCESS

SECURE RELAY CHAT SYSTEM BASED ON GOSSIP PROTOCOL USING FLUTTER

Saba Fatima

Original Article

Department of Computer Science and Engineering, Stanley College of Engineering and Technology for Women

*Corresponding Author's Email: sabafatima496@gmail.com

Abstract

The peer-to-peer (P2P) networks are made up of networked devices that share resources without the need for a centralized server. The drawbacks of centralized messaging systems include their dependence on the internet, privacy issues, and censorship. Utilizing Bluetooth and Wi-Fi Direct, the system identifies nearby devices and relays messages across multiple hops in a network, employing an efficient hybrid gossip protocol (First Push, Then Pull) for optimal message propagation. The system is built with Flutter/Dart for cross-platform compatibility and features a user-friendly interface in decentralized network, including real-time updates and device management. It emphasizes scalability, fault tolerance, and privacy, making it a practical solution for communication in challenging scenarios. The implementation uses a hybrid gossip protocol, which combines the advantages of push and pull strategies, to ensure optimal message transmission. RSA (Rivest Shamir Adleman) encryption is used for end-to-end security, and offline storage ensures delivery even when recipients are temporarily unavailable. The innovative solution offers a secure and efficient alternative to conventional messaging platforms, which makes it particularly helpful in remote locations.

Keywords: Centralized Server, Decentralized Network, Flutter/Dart, Peer-to-Peer Networks, Hybrid Gossip Protocol, Rivest Shamir Adleman (RSA) Encryption.

Introduction

Messaging systems are essential to contemporary communication, yet because they rely on centralised servers, they frequently jeopardise privacy and independence. The program uses a distributed network method in an attempt to transform messages. Using a hybrid gossip protocol and local connectivity technologies, it guarantees reliable communication even in difficult situations. Off chain storage is now the most widely used method to address the scalability and privacy security problems that the present blockchain is facing [1]. Large-scale content distribution services on the Internet have undergone a technological revolution thanks to the Peer-to-Peer (P2P) architecture. The traditional client-server design, in which every node can act as either a client or a server, is the opposite of the P2P approach. Data stored on the server is given to clients upon request in a client-server architecture [2].

A fascinating new networking platform that utilises peer-to-peer libraries included in most smartphone operating systems is gossip networks [3]. In general, the data layer, network layer, consensus layer, smart contract layer, and application layer comprise the blockchain's architecture. Among these, blockchain's decentralisation originates at the network layer [4].Each local sub-controller is connected to one sub-controller, which is selected at random from all neighbours with equal chosen probabilities, in accordance with the Gossip protocol [5].

As technology and data types continue to advance, distributed machine learning is developing quickly to keep up. In order to use the wealth of data generated on billions of end-user devices, machine learning (ML) has being gradually deployed in a distributed fashion. By training ML models privately on each participating node without explicitly sharing raw data with others, federated learning (FL), a form of networked machine learning, offers strong data privacy [6].

Gossip protocol that uses multi-factor weighting function (MFWF) that considers a number of factors, including message priority, node density, remaining energy, and the Chebyshev distance to the sink node and surrounding nodes [7]. The average number of messages needed for all nodes to query a transaction is known as the "average message complexity. The collection of various homogeneous and heterogeneous systems makes up computer networks. Depending on the medium, network can be divided into two major categories, wired and wireless [8]. Wires are used to facilitate communication in a wired computer network. In extremely complicated systems, immobility is tolerated. However, there are no cables needed for communication in a wireless network. Radio waves are used to transmit data. It facilitates mobility, allowing users to access information from any location at any time. Utilising these kinds of technologies has the benefits of increased mobility, flexibility, scalability, resilience, and affordability. However, the main disadvantages include low data transmission rates and bandwidth, poor quality of service, and increased error and delay rates [9].

A platform for gathering, connecting, and analysing donated WhatsApp chat log data is called Chat Dashboard [10]. Polyphony, an advanced chat system, which employs knowledge-based (ontology) based artificial intelligence techniques in order to support collaborative work [11]. 200 physical nodes were used in extensive trials on Emu lab to validate the P2P-PS system. Polyphony is a sophisticated chat system that supports teamwork by utilising knowledge-based (ontology-based) artificial intelligence capabilities [12].

Effective smart contracts and security gateways that use blockchain to store data in the cloud are part of the system. The centralised cloud checks the blockchain if suspicious activity is found, and the offending party is held accountable for any malicious gateway action [13].

For low latency, the P2P file sharing and searching system was implemented on the de Bruijn graph-based overlay [14]. The framework includes the following components, Dashboard Tester, an automated script that simulates users to verify that the framework is configured correctly, the Whats R R package, which parses, anonymises, and pre-processes donated WhatsApp chat logs, and the Chat Dashboard R Shiny web application, which allows users to upload, review, and securely donate WhatsApp chat logs [15].

Background and Basics- The goal of the peer-to-peer messaging software is to create a platform independent of a centralised server that is subject to legal restrictions and influenced by users from outside the system. We currently rely on apps that use central server communications, which allows them to use our personal information for their own gain despite privacy regulations and without knowing who we are. We came across situations of data breaches when the personal data of a significant number of users was leaked to hackers. Transferring the data from the central server to a distributed network would therefore be a solution. Better privacy, less reliance on the network, and exemption from central network regulations are all possible with the dispersed network. In regions that are prone to disasters, the application will be quite helpful.

Privacy-Preserving Communication: To improve user privacy and stop data breaches, create a messaging app that does not rely on central servers.

Censorship Resistance: Allow communication in settings where server access might be restricted or where censorship is likely to occur.

Disaster Resilience: Establish a dependable line of communication in places that are vulnerable to natural disasters or have poor cellular service.

Message Propagation Efficiency: To maximise message transmission among peer devices, use sophisticated gossip protocols (Push, Pull, or Hybrid).

LITERATURE SURVEY

Hongmin Gao et al. 2024. Web3.0, which emphasises the creation of a decentralised and user-controlled Internet, is the latest development in blockchain technology. Attribute-based encryption algorithms (ABE) are the mainstay of current Web 3.0 data delegation solutions, however they lack the necessary processing skills for ciphertext. Furthermore, the modified ciphertext supplied by data proxies cannot be verified using the attribute-based ciphertext transformation technique (ABCT). The main goal is to create a supervised, fine-grained attribute-based data delegation system that is optimised for Web3.0 [1].

Tao Yu et al. 2022. The study focusses on the best assured cost control issues for networked systems that are exposed to gossip scheduling protocols. The communication order of different neighbours can be determined by the gossip protocol for each subsystem. Only one nearby sub-controller will ever be chosen by the local controller of each subsystem to receive the status information from that subsystem. In order for the closed-loop interconnected system to attain exponential stability and for the cost function to be smaller than a specific maximum value, a few necessary requirements must be met. The solutions of the generated linear matrix inequality criteria are used to design all of the distributed controller gains [2].

Dishita Naik et al. 2023. In order to use the wealth of data generated on billions of end-user devices, machine learning (ML) has being gradually deployed in a distributed fashion. By training machine learning models privately on each participating node without explicitly sharing raw data with others, federated learning (FL), a form of distributed machine learning, offers strong data privacy. A global model is created by combining the local ML model updates from every node. Both centralised and decentralized/peer-to-peer methods are available for combining local model updates to create global model [3].

Xinhua Dong et al. 2024. The consortium blockchain is now the most widely utilised and researched blockchain technology across a variety of industries because to its extremely scalable and partially decentralised properties. However, the development of consortium blockchains is still hampered by performance problems including inefficient transactions and duplicated communication procedures. Consensus protocol and broadcast protocol have a significant impact on transaction efficiency in Hyperledger Fabric consortium blockchain system. In order to optimise broadcast protocols, this study presents DC-SoC, a revolutionary consortium blockchain network paradigm. The Gossip protocol optimises data transmission by establishing stable propagation structure for blockchain network through the use of the density clustering idea. Furthermore, the idea of social networks is incorporated, with node evaluations based on economic incentives and trustworthiness scores [4].

Ramakrishnan Raman et al. 2024. Achieving the best Quality of Service (QoS) in the context of Mobile Ad-Hoc Networks (MANETs) is crucial, even in the face of security risks and unpredictable network topology. To improve QoS in MANETs, this research presents a novel safe routing approach supported by a multi-constrained network feature approximation technique. The main innovation is the combination of a sophisticated feature approximation method and a multi-dimensional optimisation framework, which is designed to handle the complexities of the decentralised architecture and changing conditions of MANETs. Our suggested approach greatly improves the performance and dependability of data transmission within MANETs by concentrating on crucial QoS factors including throughput, latency, packet delivery ratio, and jitter while maintaining strong security measures [5].

Yajnaseni Dash et al. 2021. The fundamentals of the wireless networks and summary of bio-inspired ant colony-based routing algorithms are presented in the paper. The probabilistic method of determining shortest route between ant colony and its food source is the foundation of ant colony optimisation. Additionally, comparison of ant-based routing algorithm is provided, including AntHocNet (Ant agents for hybrid multipath routing), AntNet (Adaptive routing in ad hoc network), and ARA (Ant colony based routing algorithm). AntNet employs forward and backward ants to forward data

packets in a probabilistic manner. Ants in ARA create several paths on-demand between source and destination, and AntHocNet is hybrid of proactive and reactive routing elements [6].

C. Kishor Kumar Reddy et al. 2023. With the development of Internet of Things (IoT), data sharing emerged as a key feature cloud computing. Data security is still a major problem in this area, though. The study suggests a blockchain-based data-sharing framework that puts efficiency and data security first. Effective smart contracts and security gateways that use blockchain to store data in the cloud are part of the system. The centralised cloud checks the blockchain and holds the person responsible for any harmful gateway behaviour accountable if suspicious behaviour is found. Data security is ensured by the use of authentication and data sharing methods. Likewise smart contracts in blockchain employ extremely sophisticated partial decryption techniques to lessen the load on end users. Blockchain enables traceability of past acts through open and transparent monitoring to meet data restriction safety requirements. Results from experiments show that the suggested method works well for guaranteeing the security and effectiveness of information sharing across different clients. [7].

Calvin Newport et al. 2021. The peer-to-peer networking features seen in the majority of common smartphone operating systems are described by gossip algorithms in communication models. In the context, we describe and analyse a new synchronous gossip algorithm that is both simpler to operate and has faster round complexity than best-known existing solutions. It also prove new lower bound on number of rounds needed to solve gossip, which answers the small open question by proving that existing synchronous solutions are within logarithmic factors of optimal. Finally, synchronous algorithm to create novel of gossip strategy for asynchronous model that closely resembles interface of typical smartphone peer-to-peer networking library. The asynchronous strategy effectively resolves gossip by utilising novel analysis techniques. The asynchronous strategy effectively resolves gossip by utilising novel analysis techniques. It is the first successful asynchronous information distribution outcome for a peer-to-peer smartphone environment [8].

Lina Altoaimy et al. 2020. The gossip-based protocol takes into account several parameters, such as message priority, node density, residual energy, and the Chebyshev distance to nearby nodes and sink node, by using multi-factor weighting function (MFWF). Elements effects were examined in order to guide the weight function's customisation for effective data dissemination to types of IoT applications, critical, bandwidth intensive, and energy efficient applications. The performance resulting MFWFs was assessed by contrasting it with the traditional gossiping protocol and fair efficient location-based gossiping (FEL Gossiping) protocol [9].

C. Kishor Kumar Reddy et al. 2023. Maintaining attendance is crucial for tracking student attendance in institution. Every institute has a different position. Others still use antiquated paper to manually record attendance for each class hour, transfer the data to server, or use file-based method. Some institutes embraced biometric technologies for automated attendance. Unfortunately, using these tactics necessitates standing in queue for hours. Therefore, the main goal of the system is to leverage cameras that are already installed in classrooms to construct automated system that uses artificial intelligence-based student attendance monitoring on hourly basis [10].

Mehrdad Kiamari et al. 2024. In order to make mobile devices first-class citizens in consensus process, Blizzard is a distributed ledger system that uses Byzantine Fault Tolerance (BFT). Through the use of online brokers for communication between the mobile nodes and a decentralised matching system that guarantees, each node connects to predetermined number of randomly selected broker, Blizzard presents a revolutionary two-tier architecture. by examining Blizzard's performance in terms of message complexity, latency, and throughput. It demonstrates through software implementation-based experiments that Blizzard can achieve sub-second confirmation latency and throughput of several thousand transactions per second [11].

Daniele Croce et al. 2020. Community of smart buildings with energy generating and storage capabilities can automatically govern and implement the distributed demand response (DR) schemes using the Privacy-Preserving method for Over-grid. Expanding earlier Over-grid methods to enable privacy preserving data aggregation (PP-Over-grid) in order to monitor building power consumption while maintaining user privacy. The novel method combines the Secure Multi-Party Computation paradigm with a distributed data aggregation methodology [12].

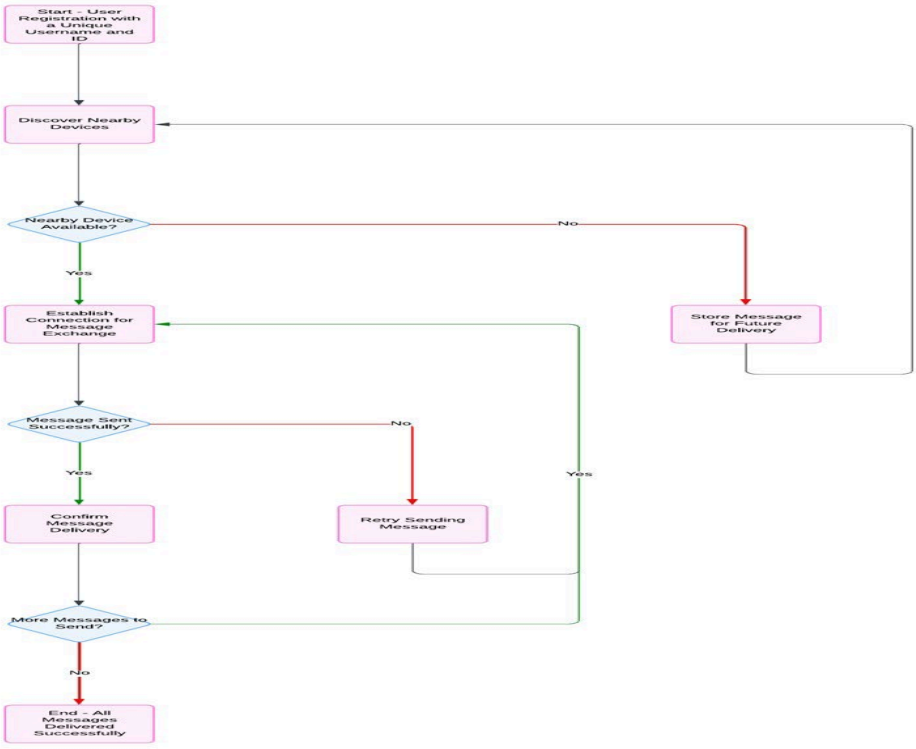
EXISTING SYSTEM

Conventional messaging apps store and transmit messages using central servers. They still have to deal with issues like censorship threats due to centralised server control, even with encryption. Possible user metadata breaches that expose

communication habits. Reliance on internet access. The effectiveness of such systems is limited by these issues, particularly in situations where privacy is a concern or in places with spotty network connection.

FLOWCHART

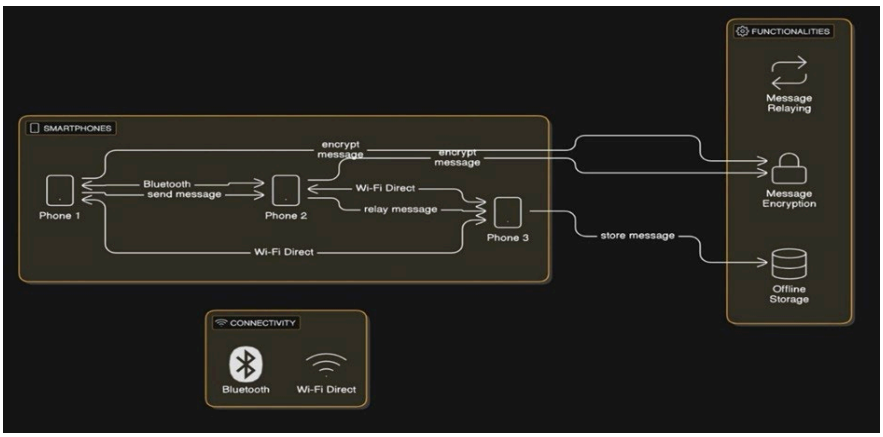
Fig 1. Flowchart



Explanation:
The system starts by registering the user with a unique username and ID, ensuring every user is distinct. It then discovers nearby devices and establishes connections to enable message exchange using the gossip protocol. If messages cannot be delivered immediately, they are stored locally and sent later when the recipient is available.

SYSTEM ARCHITECTURE

Fig 2. Bluetooth & Wi-Fi Direct Secure Messaging System



Explanation:
The Architecture illustrates peer-to-peer messaging platform. It visually represents the key components and flow, including device discovery, message transmission via the gossip protocol, offline storage, RSA encryption, and the hopping mechanism for relaying messages.

PROPOSED METHODOLOGY

The proposed system ensures **decentralized communication** by eliminating the need for a central server, allowing messages to travel directly between devices. Using a **hopping mechanism**, messages are relayed through nearby devices to reach their destination, even if the recipient is not directly connected. This system operates **internet-free**, relying solely on Bluetooth and Wi-Fi Direct for communication, making it highly effective in areas with poor or no internet connectivity. To enhance **privacy and security**, messages are encrypted end-to-end using RSA encryption, ensuring only the intended recipient can access them. Additionally, the system supports **offline messaging,** storing undelivered messages locally and retrying delivery when the recipient comes back online. Its **disaster resilience** makes it ideal for use in emergencies or remote locations, providing reliable communication even during network disruptions.
Gossip Protocol: The gossip protocol is a decentralized communication method that enables nodes in a network to share information and data without a centralized authority. It's based on how rumors spread in a social setting, where information is shared rapidly from person to person.
Push gossip protocol: When node receives a message or gossip, it periodically passes it on to other nodes, and that node is said to be infected.
All infected nodes periodically multicast to other nodes.
Pull gossip protocol: Periodically pull a few randomly selected processes for new multicast messages that you haven't received.
If there are multiple such messages, it polls a few of them randomly.
Hybrid variant: Mix of both push and pull types, push protocol is lightweighted in large groups, spreads quickly and is highly fault-tolerant.

CONCLUSION

The peer-to-peer messaging system leverages Bluetooth and Wi-Fi Direct to establish direct communication between devices, eliminating the need for central servers. It employs RSA (Rivest Shamir Adleman) encryption for secure, end-to-end message transmission. Messages are efficiently propagated using a hybrid gossip protocol (First Push, Then Pull), optimizing message delivery speed and reliability. Additionally, the system ensures offline message storage, retrying delivery when the recipient is available. These features make the system highly scalable, fault-tolerant, and ideal for use in emergency scenarios or areas with limited internet access.

References

[1] Hongmin Gao et al, “Blockchain-enabled supervised secure data sharing and delegation scheme in Web3.0”, Journal of Cloud Computing: Advances, Systems and Applications, 2024.

[2] Tao Yu et al, “Optimal guaranteed cost control for interconnected large-scale systems under networked gossip protocol”, IEEE, 2022.

[3] Dishita Naik et al, “An Introduction to Gossip Protocol Based Learning in Peer-to-Peer Federated Learning”, IEEE, 2023.

[4] Xinhua Dong et al, “DC-SoC: Optimizing a Blockchain Data Dissemination Model Based on Density Clustering and Social Mechanisms”, MDPI, 2024.

[5] Dr Ramakrishnan Raman et al, “Enhancing Quality of Service in Mobile Ad-Hoc Networks through Secure Routing with Multi-Constrained Network Feature Approximation”, IEEE, 2024.

[6] Yajnaseni Dash et al, “Nature Inspired Routing in Mobile Ad Hoc Network”, IEEE, 2021.

[7] Calvin Newport et al, “Asynchronous Gossip in Smartphone Peer-to-Peer Networks”, IEEE, 2021.

[8] Lina Altoaimy et al, "Context-Aware Gossip-Based Protocol for Internet of Things Applications", MDPI, 2020.

[9] Mehrdad Kiamari et al, Blizzard: "A Distributed Consensus Protocol for Mobile Devices", MDPI, 2024.

[10] Daniele Croce et al, "Privacy-Preserving Overgrid: Secure Data Collection for the Smart Grid", MDPI, 2020.

[11] Nikita Bhagatkar et al, "An integrated P2P framework for E-learning, Peer-to-Peer Networking and Applications", Springer, 2020.

[12] Ciprian Onofreiciuc et al, "Polyphony, a Knowledge-based Chat System Supporting Collaborative Work", Advances in Intelligent and Distributed Computing, Springer, 2020.

[13] C. Kishor Kumar Reddy et al, "A Blockchain-Based Data-Sharing Framework for Cloud Based Internet of Things Systems with Efficient Smart Contracts", IEEE ICC, 2023.

[14] C. Kishor Kumar Reddy et al, "Intelligent Systems Powered Hourly Attendance Capturing System", 7th IEEE International Conference on Trends in Electronics and Informatics, 2023.

[15] Julian Kohne et al, ChatDashboard: "A Framework to collect, link, and process donated WhatsApp Chat Log Data", Behavior Research Methods, Springer, 2023.