IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

Protecting Privacy in Peer to Peer Clouds: Anonymity Solutions

Maheen Y Quazi, Prof. Hirendra Hajare

M. Tech Scholar, Department of Computer Engineering, Ballarpur Institute of Technology, Bamni, Maharashtra, India

Assistant Professor, Department of Computer Engineering, Ballarpur Institute of Technology, Bamni, Maharashtra, India

ABSTRACT: Multi-server authentication systems streamline registration by consolidating access to multiple services, reducing the hassle of managing numerous passwords from different providers. Traditional registration methods often burden users with password memorization for each service. Multi-server authentication simplifies this by enabling real-time client authentication via public channels, thereby enhancing service accessibility. As multi-server authentication protocols advance, education seeks more efficient and adaptable authentication schemes. In this context, we propose anonymous authentication mechanisms to mitigate significant security risks like impersonation, insider attacks, and password compromise within a rational computing framework. Our approach employs the random oracle model for a rigorous security evaluation, distinguishing it from existing protocols. This comprehensive evaluation, demonstrating superior performance in terms of computational efficiency, communication, and storage costs, underscores the effectiveness of our proposed scheme in ensuring user anonymity and data encryption, particularly in multi-server scenarios.

KEYWORDS: privacy protection, peer-to-peer networks, cloud computing, data encryption, decentralized architecture, identity concealment, secure communication, privacy-preserving protocols.

I. INTRODUCTION

The Internet serves as a pivotal platform for global communication and information exchange, offering indispensable services like email, messaging, real-time traffic updates, and online forums, which significantly enhance our lives and foster diversity. However, segments of the population remain disconnected from this digital landscape, impeding their participation in this modern era of transformation.

The evolution of the Internet now advances toward the Internet of Things (IoT), a concept initially conceived in the 1990s. IoT entails linking all accessible physical devices to the Internet through tailored communication channels, thereby endowing these devices with intelligence within highly connected digital ecosystems.

These intelligent devices collaborate by sharing data, autonomously executing tasks, and amplifying human productivity and convenience. Moreover, standards and protocols for inter-device communication, particularly in the automotive sector, are being refined to accommodate the surge in vehicle numbers, especially in daily commuting scenarios. This has given rise to the Internet of Vehicles (IoV) concept, nested within the broader IoT framework, aiming to facilitate seamless information exchange among vehicles for enhanced efficiency and safety.

II. REPHRASED VANET BROADCASTING

Broadcast communication (BC) holds significant importance within VANETs, formally defined as the process of disseminating information from a source vehicle (SV) to all neighboring vehicles in the network. Given the absence of pre-designated traffic routes, BC has the capability to distribute information of public interest efficiently. It plays a crucial role in delivering time-sensitive safety messages and critical information to all vehicles in the network without discrimination. Consequently, VANET BC facilitates various applications such as advertising, traffic congestion detection, and natural disaster management systems. Moreover, establishing a BC communication system entails several fundamental steps and criteria.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

2.1 Information Packet

The transmission of information via cables or wires constitutes a significant aspect [24]. Such data exchange occurs within a network framework. In the context of VANET BC, vehicles similarly transmit network packets, termed here as information packets (Pinfo) in this study. These packets encompass diverse metrics, notably Time To Live (TTL) and OI (Other Information). TTL assigned to Pinfo denotes its lifespan, and upon expiration, the Pinfo is deemed obsolete and promptly disregarded by vehicles with any associated transmission capability. Additionally, OI encompasses distinctive and pertinent data, such as real-time traffic updates, exchanged among vehicles.

2.1 Source vehicle

A vehicle transmitting supplementary information (OI) via a pin is denoted as a source vehicle (SV) [25]. Within the Broadcast Communication (BC) system, the SV is substituted with the PINFO. The distinctive feature of pins lies in their confidentiality, as the information they convey cannot be accessed by others.

2.3 Network Coverage

In the preceding section discussing Primary Information (Pinfo), it was emphasized that a key aspect of Broadcast Communication (BC) systems is the absence of specific destination vehicles [26]. However, this characteristic presents a challenge in determining the criteria for terminating Pinfo transmission. To tackle this issue, BC systems have introduced the concept of achieving network coverage (NC). Essentially, NC for a Pinfo is achieved when the Pinfo is received by all vehicles within a network. Therefore, effective BC in Vehicular Ad Hoc Networks (VANETs) is unattainable without achieving NC.

Furthermore, the attainment of NC hinges on defining a network for the Pinfo. Depending on the type and purpose of the information being broadcast, the network may encompass varying vehicle densities, ranging from a single vehicle to thousands. For example, consider two scenarios: Pinfoa contains an advertisement for a local store, whereas Pinfob disseminates information about a road closure. Each scenario targets a distinct set of networks, reflecting the diverse purposes and audiences of the information being conveyed.

2.4 Neighbours

Wireless communication within vehicular ad hoc networks (VANETs) relies on On-Board Unit (OBU) hardware with a limited communication range, typically around 1000 meters. Consequently, vehicles within VANETs can only directly interact with their immediate neighbors. However, numerous vehicles in VANETs may be within close proximity to a standard vehicle (SV). These vehicles, commonly referred to as adjacent vehicles in this thesis, play a crucial role in disseminating essential information (Pins) throughout the VANET.

Moreover, this study focuses on multivehicle networks that extend beyond the immediate vicinity of the SV. This emphasis underscores the significance of considering communication connectivity beyond merely the vehicle's immediate neighbors, as information exchange in VANETs frequently involves multiple vehicles that are not directly in communication range.

2.5 Relay Vehicles and Retransmission

Because OBUs in VANETs restrict transmission to neighboring vehicles only, SV transmission alone cannot achieve NC without assistance from other vehicles.

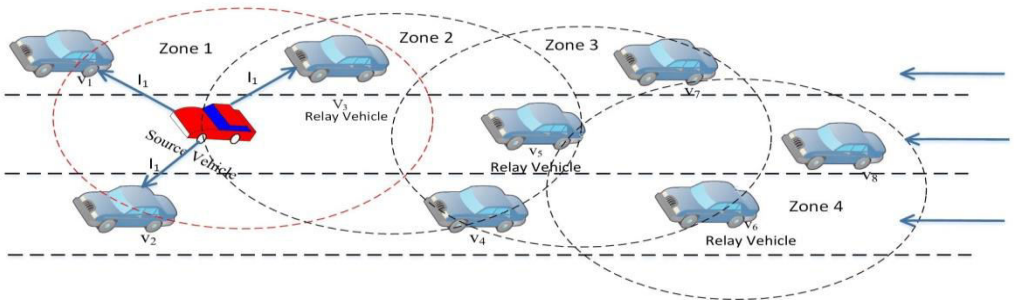

Figure 1 illustrates the dissemination of packets within a vehicular ad-hoc network.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

III. RESEARCH PROBLEM FORMULATION

This section provides an in-depth exploration of the research problem formulation, covering key terms and concepts. The research problem entails devising a Broadcast Communication (BC) system that is both secure and efficient for real-time Vehicular Ad Hoc Networks (VANETs). Within this framework, two distinct types of systems emerge: an efficient BC system (BCE) and a secure BC system (BCS).

The BCE system is responsible for the swift and effective dissemination of Primary Information (Pinfo) throughout the VANET. It focuses on optimizing the broadcasting process to ensure timely and reliable delivery of information to all relevant vehicles within the network.

In contrast, the BCS system is designed to uphold the integrity and authenticity of the broadcasted Pinfo. Its primary aim is to prevent unauthorized alterations or manipulations to the transmitted information, thereby ensuring that the received Pinfo remains unaltered and trustworthy.

Both BCE and BCS systems are crucial components in addressing the challenges associated with implementing real-time VANET systems. These challenges span various issues, from ensuring efficient and dependable communication to safeguarding the security and integrity of transmitted data. Subsequent subsections will delve deeper into these BC systems and the associated challenges inherent in deploying real-time VANET systems.

3.1 Efficient Broadcast Communication System

A Broadcasting Communication Efficiently (BCE) entails methodologies and techniques directed towards disseminating Pinfo (information packets) to all vehicles within a network before the Time To Live (TTL) expires. The distinctive features of a BCE are elucidated in detail below:

Time To Live (TTL):

An expired TTL for a Pinfo is essential to prevent its transmission, thereby averting delays and congestion resulting from mixing with Pinfo possessing valid TTLs. The revised Equation 1.6 and its associated equations, incorporating TTL, are presented below:

$$N_C := \begin{cases} 1, & \text{if } BC_{efficiency} = 1 \ \& \ TTL = valid \\ 0, & \text{else ,} \end{cases} \tag{1.6}$$

Network Coverage (NC):

Attaining Network Coverage (NC) is vital for establishing Broadcasting Communication Efficiently (BCE). Hence, the BCE equation can be formulated as follows:

$$BC_E := N_C, \tag{1.1}$$

$$N_C := \begin{cases} 1, & \text{if } BC_{efficiency} = 1 \\ 0, & \text{else ,} \end{cases} \tag{1.2}$$

$$BC_{efficiency} := \frac{N_C^t}{|\mathcal{V}|}, \tag{1.3}$$

$$N_C^t := \sum_{i=1}^{|\mathcal{V}|} R_i^t, \tag{1.4}$$

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

In this equation: BCefficiency denotes the efficiency of Broadcasting Communication (BC) at time t. To attain Network Coverage (NC), BCefficiency must equal 1. NCt signifies the Network Coverage at time t. V represents a set of vehicles, expressed as V = {1, 2, 3, ..., Vn}. Ri indicates whether the Pinfo has been received by each vehicle i or not, where i ranges from 1 to the total number of vehicles, denoted as |V|. Formally, Ri is defined as follows:

$$R_i := \begin{cases} 1, & \text{if } PacketRecieved \\ 0, & \text{if } PacketNotRecieved. \end{cases} \tag{1.5}$$

Data Transmission:
A vehicle should initiate transmission only if one or more vehicles in its immediate vicinity have not received the Pinfo. Moreover, each vehicle possesses a set of transmission states, denoted as T, comprising values of 1 and 0. The value 1 indicates a transmission state (ST), whereas 0 denotes an idle state. Additionally, at any given moment, a vehicle will have a specific transmission state Ti, where i ranges from 1 to the total number of vehicles, denoted as |V|. To incorporate Ti, Equation 1.1 is modified as follows:

$$BC_E := N_C \times T_S, \tag{1.7}$$

$$T_S := \prod_{i=1}^{|\mathcal{V}|} T_i, \tag{1.8}$$

$$T_i := \begin{cases} 1, & \text{if } R_N = 0 \\ 0, & \text{otherwise }, \end{cases} \tag{1.9}$$

$$R_N := \prod_{i=1}^{|\mathcal{V}^{\mathcal{N}}|} R_i, \tag{1.10}$$

IV. SCOPE

Strategies aimed at selecting Relay Vehicles (RVs) to mitigate the Broadcast Storm Problem (BSP) have been proposed in previous research, which are discussed in subsequent chapters. However, these strategies often lack optimization processes or utilize optimization parameters inefficiently. Therefore, this thesis introduces a Broadcasting Communication Efficiently (BCE) system based on a novel optimization RV selection mechanism. Additionally, the thesis introduces a layer-based architecture to facilitate Broadcast Communication Secure (BCS). The design of these strategies supports Vehicle-to-Vehicle (V2V) communication in both highway and urban multi-hop environments. The primary objective of this research is to establish secure information sharing through transmission and retransmission processes in a Broadcast Communication (BC) VANET system. The process of selecting information for dissemination by a Source Vehicle (SV) is beyond the scope of this research.

V. LITERATURE SURVEY

5.1 Introduction:
The problem statement and objectives involve devising methodologies to mitigate the Broadcast Storm Problem (BSP) and enhance communication security. Achieving this goal requires the introduction and optimization of parameters governing Broadcast Communication (BC) in VANETs. Introducing and refining these parameters necessitates a focus on gathering empirical evidence from numerical and simulation data.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

5.2 Research Methodology

The research process adheres to a quantitative research methodology due to its ability to design, investigate, and establish relationships between parameters governing BC. Quantitative research methodology is formally defined as a systematic empirical investigation utilizing statistical, mathematical, and/or computational techniques [34]. Furthermore, the research process is divided into three incremental phases, as outlined below.

Analysis:

A comprehensive literature review is conducted to identify research achievements and challenges within the targeted research field. Previous research achievements are assessed by analyzing parameters utilized to establish an efficient and secure Broadcast Communication (BC) system in VANETs. Conversely, challenges pinpoint research areas requiring further exploration for optimal solutions. These activities are conducted within a specialized phase known as analysis.

Design:

The design phase encompasses the process of creating and developing architectures/systems. This phase involves exploring, observing, and establishing relationships between different parameters governing Relay Vehicle (RV) selection or secure communication to establish Broadcasting Communication Efficiently (BCE) and Broadcast Communication Secure (BCS) systems. The research gap identified in the previous phase plays a crucial role in guiding design and development activities.

Verification:

In this phase, the proposed designs are implemented in a Python environment [35]. Python is chosen due to its widespread use in scientific research and the availability of open-source libraries offering efficient mathematical capabilities [36]. The results obtained from Python implementation are then compared with those of state-of-the-art methodologies in VANET BC.

5.3 Key Literature Findings

This section outlines the key findings derived from the review of previous research studies, as follows:

There are a number of relay vehicle selection mechanisms proposed in the previous research studies that solve only one-hop or two-hop BC VANETs, therefore lacking capability to handle complex multi-hop BC systems.

Different relay vehicle selection mechanisms processes depend on predefined information parameters and their associated values that require accurate information for efficient performance of the system. These mechanisms are mostly dependent on GPS, which has the tendency to fail specially in urban environment comprising of high-rise buildings.

The ineffectiveness of previously proposed mechanisms stems from the reliance on outdated information within the relay vehicle selection mechanism (RVSM).This is caused by complex date gathering and time required by analytical engine to calculate information provided to the relay vehicle selection mechanism.

In the previous research, in order to establish a secure BC system, generally a centralised mechanism is required. This centralised mechanism can cause a single point failure. Also, the wireless communication connection between a centralised system and vehicles may not be guaranteed all times.

Some of the current research studies include Road Side Units (RSUs) in their model. Although, RSUs provide extra benefit in the model, their deployment is expensive in real world. They also may not be deployed everywhere due to geographical limitations.

Security Analysis:

This section provides both informal and formal security analyses to showcase the safety and security of the proposed system against various potential attacks.

Informal Security Analysis:

Assumptions about user anonymity: Unlike many authentication schemes for multi-server environments, where the server cannot identify the user initiating the login request, our protocol maintains a dynamic pseudo-identity (PIDu) when the authentication request is sent to Sj. By utilizing only the user's identity (IDu), the server's private key can be removed, ensuring user anonymity and traceability.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

against replay attacks: In the case of replay attacks, where an adversary intercepts messages to deceive legitimate users, our protocol ensures security by generating two unique challenge-responses (Cu and Dj) for each session. Even if the adversary obtains parameters, they cannot execute an attack due to the uniqueness of the challenges.

Ensuring known-key security: The protocol guarantees known-key security by safeguarding the confidentiality of the private key, even if the session key is compromised, thus preventing adversaries from accessing parameters derived from the session key.

Protection against smart card attacks with offline dictionaries: Attempts by adversaries to guess a password (PWu) from known parameters (Yu and Fu) in smart card attacks, mitigated through offline dictionary attacks, are thwarted by the system configuration, making such attacks computationally infeasible within polynomial time using the smart card.

Mutual authentication: Our enhanced system ensures mutual authentication among legitimate stakeholders, facilitating prompt detection of potential attacks, including counterattacks.

Defense against verifier stolen attacks: Adversaries attempting to exploit data stored on the server side or compromise user privacy cannot masquerade as legitimate users because the protocol provides mutual authentication without managing storage on the server-client side.

Existing System
In current systems, authentication and key agreement mechanisms for peer-to-peer cloud systems can differ based on specific implementations and protocols. Nonetheless, I can offer an overview of several existing approaches and technologies utilized in this context:

Public Key Infrastructure (PKI):
Certain peer-to-peer cloud systems employ a PKI-based strategy for authentication and key agreement. Within this framework, peers receive public and private key pairs from a trusted certificate authority (CA). Peers utilize their private keys to sign messages and authenticate themselves to other peers. The verification of signatures and the establishment of secure communication channels hinge upon the CA's trusted certificates.

Anonymous Credentials:
Anonymous credential systems like U-Prove and Idemix offer a means to attain anonymous authentication within peer-to-peer cloud systems. In this setup, peers receive anonymous credentials from a trusted authority, enabling them to authenticate with other peers without divulging their true identities. These credentials include cryptographic proofs that validate their legitimacy without exposing the underlying identity information.

Identity-Based Encryption (IBE):
Identity-based encryption schemes like Boneh-Franklin and Waters offer a method for ensuring secure communication within peer-to-peer cloud systems. In this setup, peers can encrypt messages utilizing the recipient's identity, serving as the public key. Subsequently, the recipient can decrypt the messages using their private key, securely derived from their identity.

While these existing approaches and technologies serve as fundamental pillars for authentication and key agreement in peer-to-peer cloud systems, the implementations may vary, and additional mechanisms may be integrated to fulfill the unique requirements of each system. It is crucial to meticulously design and assess the security, privacy, scalability, and efficiency aspects when implementing these solutions in practice.

Proposed System
Several relay vehicle selection mechanisms proposed in prior research studies are designed to address only one-hop or two-hop Broadcast Communication (BC) VANETs, thus lacking the capability to handle complex multi-hop BC systems.

Various relay vehicle selection mechanisms rely on predefined information parameters and their associated values, necessitating accurate information for efficient system performance. These mechanisms often rely heavily on GPS, which can be prone to failure, especially in urban environments with high-rise buildings.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

The outcomes of previously proposed mechanisms are inefficient due to reliance on outdated information within the relay vehicle selection mechanism (RVSM). This issue stems from the complexity of data gathering and the time required by the analytical engine to compute information for the relay vehicle selection mechanism.
While some current research studies incorporate Road Side Units (RSUs) into their models to provide additional benefits, their real-world deployment can be costly. Additionally, RSUs may not be deployed universally due to geographical limitations.

VI. SYSTEM DESIGN

Class Diagram:
Class diagrams illustrate the static structure of the system.
They visualize the classes, along with their attributes, methods, and the associations between them.
Class diagrams elucidate the arrangement of the system's classes and their interactions.

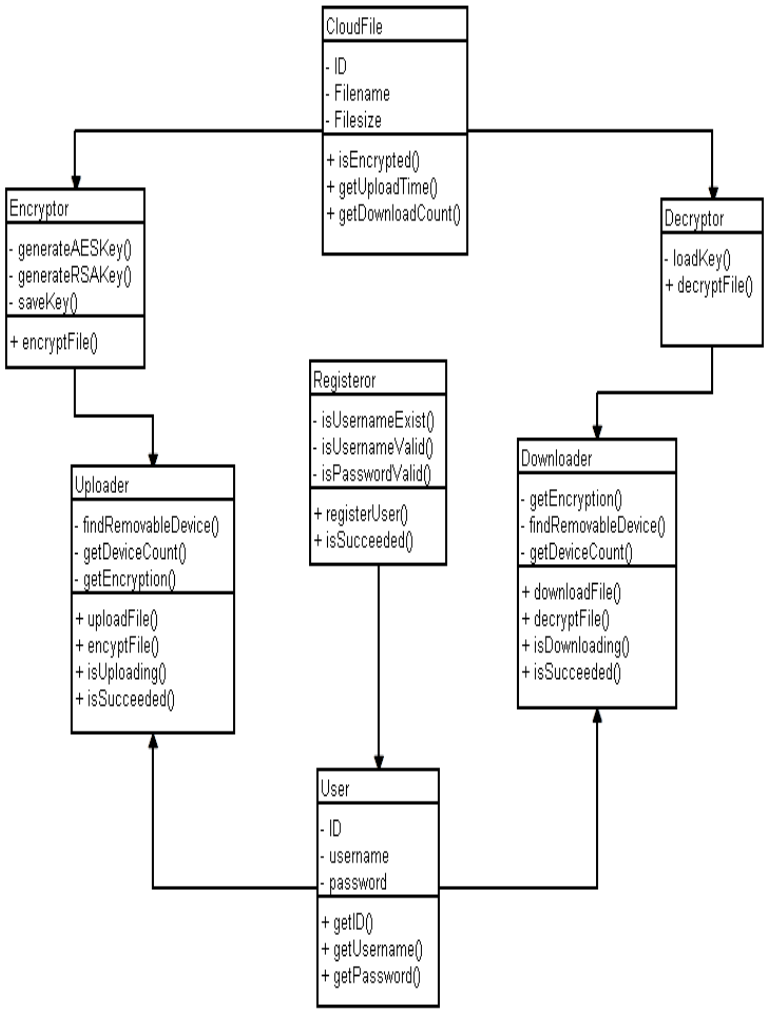

Fig 2 : Class Diagram illustrating protecting privacy in peer to peer clouds anonymity solutions

Sequence Diagram:
Sequence diagrams illustrate the dynamic behavior of the system, focusing on the interaction between objects or components over time.
They depict the sequence of messages exchanged between objects and the sequence of their execution.
Sequence diagrams aid in visualizing the flow of control and data during a particular scenario or use case.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

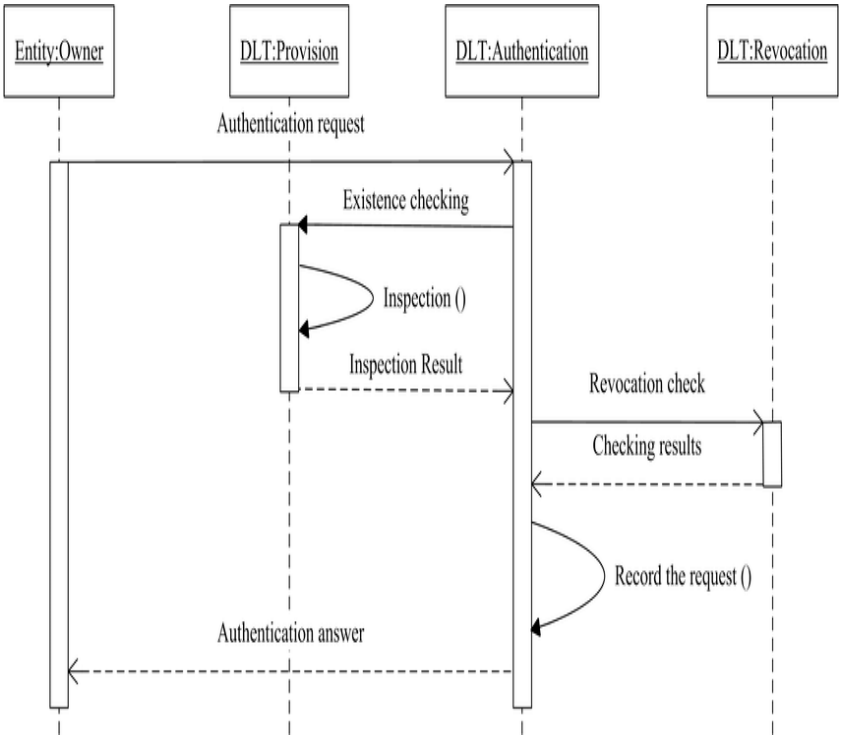

Fig 3 : Sequence diagram of protecting privacy in peer to peer clouds anonymity solutions

VII. RESULT

Screen shots:

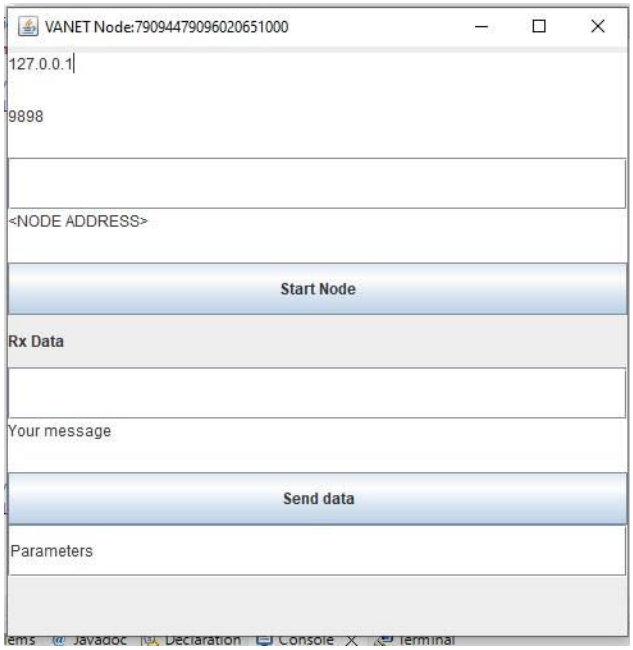

Figure 4: Sender of protecting privacy in peer to peer clouds anonymity solutions

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

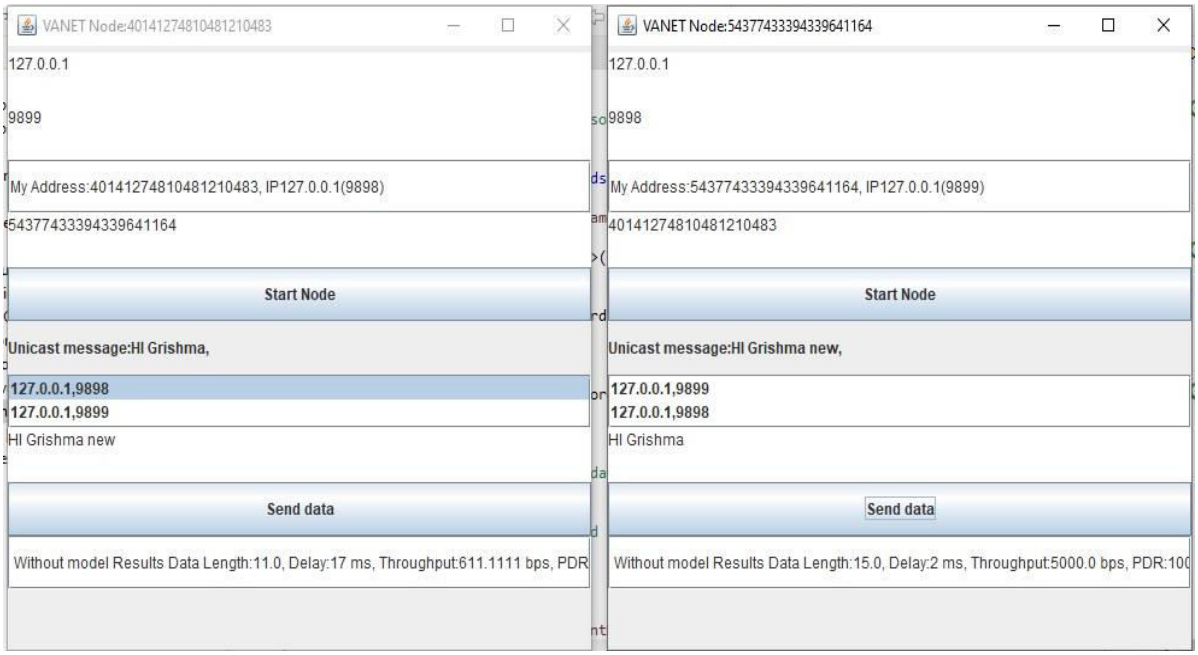

Figure 5: Sender and Receiver Node of protecting privacy in peer to peer clouds anonymity solutions

VIII.CONCLUSION

In essence, authentication and specialized contract mechanisms serve as crucial components in peer-to-peer cloud infrastructure, facilitating secure and anonymous communications among peers through robust security protocols, privacy protection mechanisms, and cryptographic algorithms. By fostering a secure environment, the system empowers users to engage independently and establish secure communication channels. The proposed system offers numerous advantages over existing solutions, particularly in terms of enhanced security, privacy protection, scalability, connectivity, and user-friendliness.

The proposed tool amalgamates features like anonymous authentication, secure key agreement protocols, and privacy enhancement technologies to address current system shortcomings. The software requirements specification delineates active and passive system requirements, while external interface requirements stipulate interfaces with external systems. Security, privacy, scalability, and adherence to system objectives and principles guide the design process. UML diagrams serve as visual aids, elucidating usability, class hierarchy, sequential actions, interconnected components, and hierarchies. These diagrams enhance comprehension of organizational structures, practices, and relationships, thereby refining communication, planning, and documentation processes.

Aligned with design objectives, principles, and module specifications, the specialized authentication and contracting mechanisms are poised to deliver a secure, privacy-protective, scalable, and user- friendly solution for peer-to-peer cloud systems. Ensuring confidentiality, integrity, and authenticity of user data and communications while preserving privacy is paramount. Seamless collaboration between peers is prioritized to ensure the system's seamless operation.

REFERENCES

1. Bogdan Alexe, Thomas Deselaers, and Vittorio Ferrari, “What is an object?”, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2010.
2. Sean Bell, Paul Upchurch, Noah Snavely, and Kavita Bala, “Material recognition in the wild with the materials in context database.” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,3479-3487, 2015“.
3. Design of a Convolutional Neural Network Based Smart Waste Disposal System.Thung, Gary and M. Yang. “Classification of Trash for Recyclability Status.” (2016).

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305065 |

4. C. Liu, L. Sharan, E. H. Adelson, and R. Rosenholtz, "Exploring features in a bayesian framework for material recognition," in Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on. IEEE, 2010, pp. 239–246.
5. George E Sakr, Maria Mokbel, Ahmad Darwich, Mia Nasr Khneisser and Ali Hadi, "Comparing Deep Learning And Support Vector Machines for Autonomous Multidisciplinary Conference.
6. S. Kaza, L. Yao, P. Bhada-Tata, and F. Van Woerden, What a Waste 2.0: A Global Snapshot of Solid Waste Management to 2050. The World Bank, 2018.
7. "Convolutional networks and applications in vision," in Proceedings of 2010 IEEE International Symposium on Circuits and Systems, Paris, France, pp. 253–256, May 2010. doi: 10.1109/ISCAS.2010.5537907.
8. N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," in 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), San Diego, CA,USA, vol. 1, pp. 886–893, 2005. doi: 10.1109/ CVPR.2005. 177.
9. Recognition," in arXiv:1409.1556 [cs], San Diego, CA, USA, pp. 1–14, May 2015, [Online]. Available: http://arxiv.org/abs/1409.1556 [Accessed: Sep. 27, 2019].
10. K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, pp. 770–778, Jun. 2016. doi: 10.1109/CVPR.2016.90.
11. C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," ACM Trans. Intell. Syst. Technol., vol. 2, no. 3, pp. 1– 27, Apr. 2011. doi: 10.1145/1961189.1961199.
12. M. Yang and G. Thung, "Classification of Trash for Recyclability Status," Stanford University, CS229, 2016.
13. C. Bircanoglu, M. Atay, F. Beser, O. Genc, and M. A. Kizrak, "RecycleNet: Intelligent Waste Sorting Using Deep Neural Networks," in 2018 Innovations in Intelligent Systems and Applications (INISTA), Thessaloniki, p.1–7, Jul. 2018. doi: 10.1109/INISTA.2018.8466276.
14. H. Khan, "Transfer learning using mobilenet," 2019. [Accessed Sep. 23, 2019]. Kochalko, D. Making the unconventional conventional: How blockchain contributes to reshaping scholarly communications. *Inf. Serv. Use* 2019, *39*, 199–204. [CrossRef].
15. Leelasantitham, A. A Business Model Guideline of Electricity Utility Systems Based on Blockchain Technology in Thailand: A Case Study of Consumers, Prosumers and SMEs. *Wirel. Pers. Commun.* 2020, *115*, 3123–3136. [CrossRef].
16. Chen, T.; Alsafasfeh, Q.; Pourbabak, H.; Su, W. The Next-Generation U.S. Retail Electricity Market with Customers and Prosumers—A Bibliographical Survey. *Energies* 2017, *11*, 8. [CrossRef].
17. Da Silva, F.R.; Teixeira, R.V.G. The Use of the Blockchain Protocol by Public Administration as an Accomplishment of Efficiency in the Public Service. *J. Public Adm. Gov.* 2018, *8*, 333–343. [CrossRef].
18. Tan, S.; Wang, X.; Jiang, C. Privacy-Preserving Energy Scheduling for ESCOs Based on Energy Blockchain Network. *Energies* 2019, *12*, 1530. [CrossRef].
19. Noor, S.; Yang, W.; Guo, M.; van Dam, K.H.; Wang, X. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy* 2018, *228*, 1385–1398. [CrossRef]

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details