IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE CONNECTIONS : ANONYMITY FOR PEER TO PEER CLOUDS

Miss Maheen Y. Quazi, Mr. Hirendra Hajare
M.Tech scholar, Assistant Professor
[1]Computer Science and Engineering,
[1]Ballarpur Institute of Technology, Ballarpur, India

Abstract: Multi-server authentication systems offer greater value through a single registration, and make it easier to access multiple services from trusted servers through a single agent Traditional registration methods often hinder users due to the burden of remembering multiple passwords from each service provider. Multi-server authentication simplifies this process by enabling real-time client authentication over public channels, increasing the availability of services. With the advent of more multi-server authentication protocols, education continues to search for more efficient and flexible authentication schemes. In this context, we offer anonymous authentication mechanisms designed to mitigate major security threats such as impersonation, insider attacks, and password compromise, all in place in a rational computing system Our approach uses the random oracle model for a more formal security evaluation, compared to existing protocols This comprehensive evaluation, which reveals better performance in terms of computing power, . in terms of communication and storage costs highlights the effectiveness of our proposed scheme in ensuring anonymity and encryption of users especially in multi-server scenarios plant.

Index Terms - Secure Connections, Anonymity, Peer-to-Peer, Cloud Computing, Privacy Protection, Data Security, Distributed Systems, Confidentiality, Authentication, Trust Management

I. INTRODUCTION

The Internet acts as an important platform for communication and information sharing [1], providing transformational services such as email, messaging, traffic updates, online forums, which greatly affect our lives and make them better for global people quantitative growth Dependent on diversity They remain disconnected from the digital realm, hindering their participation in this modern transformation.

The next stage of Internet development lies in the concept of the Internet of Things (IoT), first conceived in the 1990s, which refers to connecting all available physical devices to the Internet This connection requires connectivity uses customized communications [4 – , transforming devices into intelligent services in Internet environments with high internet usage

These intelligent devices share information, perform tasks automatically, increase human productivity and comfort [8], and develop standards and procedures for communication between intelligent devices including vehicles The role of vehicles is directly related to the increasing number of vehicles especially in daily commute [9, 10 and the concept of the Internet of Vehicles (IoV) to address these challenges emerged in the IoT framework in [11] . , which aims to establish and organize information exchange between vehicles [12,13].

II. VANET broadcasting

Broadcast communication (BC) stands as an important feature in VANETs, formally defined as the process of distributing information from a source vehicle (SV) to all neighboring vehicles in the network in Given the absence of pre-designated traffic, BC has the power to distribute information of public interest. It can provide critical time-sensitive safety messages and critical safety messages for all vehicles in the network, regardless of discrimination. As a result, VANET BC paves the way for applications such as advertising, traffic congestion detection, and natural disaster management systems. Additionally, there are a number of basic steps and criteria for setting up a BC communication system, including:

2.1 Information Packet

The transmission of information through cables or cables stands as an important feature [24]. These messages take place in a network format. In the case of VANET BC, vehicles also send network packets, which in this research are referred to as information packets (Pinfo). Pins include various statistics, including Time To Live (TTL) and OI (Other Information). The TTL assigned to Pins indicates its age. When the TTL expires, the PINFO is considered expired and is immediately abandoned by vehicles with any associated transmission function Furthermore, the OI contains unique and accurate information, such as traffic updates, that are shared between vehicles.

2.2 Source vehicle

A vehicle that transmits an additional information (OI) in the form of a pin is referred to as a source vehicle (SV) [25] . In the Broadcast Communication (BC) system, the SV is exchanged with the PINFO. The uniqueness of pins is the fact that others can't find the information.

2.3 Network Coverage

In the previous section discussing Primary Information (Pinfo), it was highlighted that a crucial aspect of Broadcast Communication (BC) systems is the absence of specific destination vehicles [26]. However, this characteristic poses a challenge in determining the criteria for terminating Pinfo transmission. To address this issue, BC systems have introduced the concept of achieving network coverage (NC). Formally, NC for a Pinfo is attained when the Pinfo is received by all vehicles within a network. Thus, without achieving NC, effective BC in Vehicular Ad Hoc Networks (VANETs) is not feasible.

Moreover, the attainment of NC is contingent upon the definition of a network for the Pinfo. Depending on the type and purpose of the information being broadcast, the network can comprise varying vehicle densities, ranging from a single vehicle to thousands. For instance, consider two scenarios: Pinfoa contains an advertisement for a local store, while Pinfob broadcasts information about a road closure. Each of these scenarios targets a distinct set of networks, reflecting the differing purposes and audiences of the information being disseminated.

2.4 Neighbours

Wireless communication in vehicular ad hoc networks (VANETs) is carried out by On-Board Unit (OBU) hardware with a limited communication range, typically around 1000 meters and consequently, the vehicle under VANET can only interact directly with its instant neighbors . However, there are many vehicles in VANETs that may be in the immediate vicinity of a conventional vehicle (SV). These vehicles, commonly referred to as adjacent vehicles in this thesis, play an important role in the distribution of key information (Pins) throughout a VANET

Furthermore, this study focuses on multivehicle networks that extend beyond the immediate reach of the SV. This emphasis recognizes the importance of considering communication connectivity beyond just the vehicle's immediate neighbors, as information sharing in VANETs often involves multiple vehicles that are not in a direct communication path.

2.5 Relay Vehicles and Retransmission

Due to the restriction of OBUs in VANETs, which only allow VS transmission to neighboring vehicles, SV transmission alone cannot achieve NC without assistance from other vehicles.

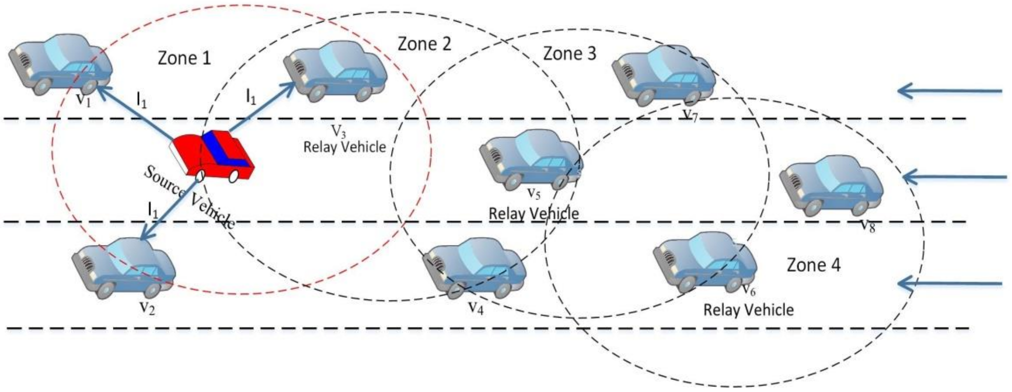


Figure 1: Dissemination of packets within a vehicular ad-hoc network

III. Research Problem Formulation

This section delves into a comprehensive discussion regarding the formulation of the research problem, encompassing pertinent terms and concepts. The research conundrum necessitates the development of a secure and efficient Broadcast Communication (BC) system tailored for real-time Vehicular Ad Hoc Networks (VANETs). Within this context, two distinct types of systems emerge: an efficient BC system (BCE) and a secure BC system (BCS).

The efficient BC system, BCE, is tasked with the effective and expedient 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.

Conversely, the secure BC system, BCS, is geared towards safeguarding the integrity and authenticity of the broadcasted Pinfo. Its primary objective 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 integral components in addressing the challenges encountered in implementing real-time VANET systems. These challenges encompass a wide array of issues, ranging from ensuring efficient and reliable communication to guaranteeing the security and integrity of transmitted data. The subsequent subsections will delve deeper into these BC systems and the associated problems inherent in deploying real-time VANET systems.
\

3.1 Efficient Broadcast Communication System

A BCE, or Broadcasting Communication Efficiently, encompasses methodologies and techniques aimed at distributing Pinfo (information packets) to all vehicles within a network before the Time To Live (TTL) expires. The notable characteristics of a BCE are elaborated upon in detail below:

- **Network Coverage:**

  Achieving Network Coverage (NC) is a crucial aspect for establishing a Broadcasting Communication Efficiently (BCE). Therefore, the BCE equation can be formulated as follows:

$$BC_E := N_C, \qquad (1.1)$$

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

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

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

In this equation:

BCefficiency represents the efficiency of Broadcasting Communication (BC) at time t. To achieve Network Coverage (NC), BCefficiency must equal 1. NCt represents the Network Coverage at time t. V is a set of vehicles, denoted as V = {1, 2, 3, ..., Vn}. Ri is a value indicating whether the Pinfo has been received or not by each vehicle i, where i = {1, 2, ..., |V|}. Formally, Ri is defined as follows:

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

- **Time To Live:**

An expired TTL for a Pinfo should prevent its transmission to avoid delays and congestion caused by mixing with Pinfo having valid TTLs. The updated Equation 1.6 and its related equations, incorporating TTL, are provided below:

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

- **Transmission:**

A vehicle should transmit only if one or more vehicles in its immediate neighbors have not received the Pinfo. Additionally, a vehicle has a set of transmission states, denoted as T, consisting of 1 and 0. The value 1 signifies a transmission state (ST), while 0 represents an idle state. Furthermore, at any given instance of time, a vehicle will have a single transmission state Ti, where i = {1, 2, ..., |V|}. To incorporate Ti, Equation 1.1 is updated as follows:

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

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

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

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

Where TS represents the product of transmission states of all vehicles. Additionally, RN denotes the packet received by all neighboring vehicles. Finally, VN is the set of neighboring vehicles of a vehicle v, defined as follows:

$$\mathcal{V}^{\mathcal{N}} = \{1, 2, ...V_N^N\}. \tag{1.11}$$

The above-mentioned three salient features form a blind retransmission system, indicating that the feature list of a Broadcasting Communication Efficiently (BCE) is incomplete. This blind retransmission system either lacks an efficient relay selection methodology or employs an inefficient one, resulting in unnecessary retransmissions. Relay Vehicle (RV) selection is the process of choosing RVs to retransmit the original Pinfo to achieve Network Coverage (NC). Furthermore, the significant consequence of unnecessary retransmissions by RVs is network congestion, which is known as the Broadcasting Storm Problem (BSP) [29–31]. BSP leads to network delays and the transmission of outdated or irrelevant Pinfos.

BSP is typically observed in multi-hop environments comprising multiple vehicles acting as RVs within the same neighborhood to retransmit to vehicles that haven't received the Pinfo. To address BSP, a BC system may opt for a strategy of no retransmission. However, this strategy fails to achieve NC in multi-hop environments. Another approach to mitigate BSP is the design and development of optimized mechanisms for RV selection, termed Optimal RV Selection (ORVS), which constitutes the fourth salient feature of the BC system.

$$\mathcal{V}^* := \{v \in \mathcal{V} | S_i(v)\} \tag{1.12}$$

where,

$$|\mathcal{V}^*| \geq 0, \tag{1.13}$$

The Optimal RV Selection (ORVS) should be capable of limiting the number of retransmissions to prevent the Broadcasting Storm Problem (BSP) while ensuring that the Pinfo achieves Network Coverage (NC). Let's define a set of optimized RVs as \(V^*\) using a specific strategy \(S\). Mathematically, this can be defined as:

$$BC_E := N_C \times T_S \times BSP, \tag{1.14}$$

$$BSP := \begin{cases} 0, & \text{if } |V| < N_R \\ 1, & \text{otherwise .} \end{cases} \tag{1.15}$$

\

where NR represents the number of retransmissions exhibited in a VANET for the purpose of propagating a Pinfo to achieve Network Coverage (NC).

IV. Research Aims and Objectives

The focus of this study, as described in the previous section, is to establish broadcast communication (BC) in vehicular ad hoc networks (VANETs) Objective to contribute to the development and improvement of broadcast vehicular communication, which is the basis for future studies in the Internet of Vehicles (IoV). It introduces the methods. The following information is provided to clarify the objectives of this thesis.

1. Review the results of previous studies on performance metrics including rate of retransmission (NR), network coverage (NC), and NC time (NCT).
2. Developing design principles to guide the construction of an ORVS instrument to produce a BCE capable of reducing redispersion and achieving NC.
3. Develop and develop a multi-objective genetic algorithm (MOGA) based on design principles to construct BCE in highway and urban environments.
4. Construct evolutionary game (EG) models to further establish the BCE and reinforce the validity of the proposed design principles.
5. Identify security threats that can compromise PINFO security and spread modified PINFOs in BC.
6. Evaluate and identify differences in previously proposed Broadcast Communication Secure (BCS) algorithms based on their effectiveness in detecting PINFO and faulty vehicle changes.
7. Develop a BCS system that can detect changes in PNFO and idle vehicles without triggering the BSP in BC

v. Literature Survey

5.1 Introduction

The selection of an appropriate research method depends on the analysis and problem statement in terms of the thematic objectives outlined in the previous sections. The problem statement and objectives revolve around identifying ways to mitigate the broadcast storm problem (BSP) and enhance network security. To this end, parameters governing broadcast control (BC) in vehicular ad hoc networks (VANETs) are determined and optimized. This process of parameter identification and refinement requires a focus on collecting empirical evidence through numerical analysis and simulation data.

5.2 Research Methodology

This topic adopts a quantitative analytical approach due to its ability to design, analyze, and establish relationships among the parameters governing propagation control (BC) in vehicular ad hoc networks (VANETs) Quantitative analysis is an analysis of they have been systematically computed, computed, and/or developed by computer methods [34] . The research process is divided into three stages as described below.

Research: This phase involves a comprehensive literature review to identify research achievements and challenges in the relevant area. It is done by analyzing the earlier research for efficient and secure

BC systems in VANETs. At the same time, challenges have been identified in areas where further research is needed in order to find improved solutions. This phase is unique as "research".

Design: The design phase encompasses the development of architectures and systems. Here, the exploration, observation, and establishment of relationships between different parameters governing either Roadside Unit (RV) selection or secure communication to establish Broadcast Control Efficiency (BCE) and Broadcast Communication Security (BCS) are pivotal. The research gap identified in the analysis phase informs and guides design and development activities.

Evaluation: In this phase, the proposed framework is implemented in Python environment [35]. Python has been chosen because of its widespread use in scientific research and the availability of open source libraries providing efficient mathematical computation and the results of using Python are then compared to state-of-the-art methods in of the VANET BC.

This chapter provides a comprehensive literature review of the research topics discussed in the thesis, with a particular focus on VANETs BCE and BCS as discussed in Chapter 1. The discussion revolves around the development of BCE of the alternative by identifying it by applying the optimal roadside object selection (ORV S). machinery The vehicle. Consequently, the main focus and main contribution of this chapter is research and preliminary analysis of RV selection methods for Broadcast Storm Problem (BSP) mitigation and analysis of protection information and security policies/procedures related to VANET BC. The remainder of this chapter is organized as follows: Previous research demonstrating RV selection methods in multi-hop environments to combat BSP is discussed in Section 2.1, while the literature on security issues and security architecture/ . the methods used to solve the VANET BC Section concept 2.2 have been developed.

5.3 Security in VANET Broadcast Communication

The second objective of this thesis is to enhance the broadcast communication security (BCS) in a vehicular ad hoc network (VANET) multi-hop environment. Addressing some key security challenges in VANETs, such as spoofing, ID exposure, and Sybil attacks [56–63] is essential. Therefore, the purpose of this section is to provide a comprehensive review of proposed strategies aimed at mitigating these security challenges and establishing secure networks in VANET BC environments.

In [64], a security system using blockchain technology is proposed. This system is based on the Internet and centralized authentication, using blockchain for distributed trust management. When a vehicle shares information with a road unit (RSU) for reporting purposes, it must also upload its real-time traffic status record. This tag is created by a vehicle approaching the Central Traffic Vehicle (CTV). RSU score calculates a reliability value based on the distance between the vehicle and the CTV, it often chooses to block malicious vehicles or systems to eliminate widespread malicious traffic but due to the reliance on centralized systems, such protection systems this is not applicable in the absence of RSU. Often, especially on highways, RSUs may not exist, leaving V2V connectivity as the only option.In [65], a novel public blockchain model is proposed to ensure security and accuracy in disseminating Primary Information (Pinfo). This public blockchain maintains a shared database among all vehicles in the network, defined within the boundaries of a country. Vehicles verify the authenticity of messages based on the database's information regarding location, timestamp, and message authenticity. However, this paper does not clearly establish how message authenticity is determined. Additionally, although the proposed blockchain is decentralized, it still relies on RSUs and the Internet.

In [66], blockchain technology is proposed to establish an anonymous reputation system in VANETs. This methodology utilizes vehicle trustworthiness to prevent malicious attacks and anonymize vehicle information for privacy concerns. However, like other blockchain-based security implementations in VANETs, this approach also depends on RSUs and the Internet.

In another approach, presented in [65], a secure architecture relying on a Trusting Authority (TA) and RSUs is proposed for transmitting Pinfo securely. Each packet and the transmitting vehicle's trustworthiness are established through a TA, while RSUs facilitate communication between the TA and vehicles. However, this system is centralized and reliant on RSUs, making it unsuitable for V2V multi-hop environments lacking RSUs.

The research methods proposed in the literature reviewed rely heavily on RSUs and centralized authorities/systems. While centralized systems offer advantages in resource management, they also present a single point of failure, which can be mitigated by decentralizing the system. However, the dynamic nature of VANETs means that the availability of a connection to a centralized system is not guaranteed. Additionally, RSUs are costly and cannot be deployed in every geographic location. Therefore, there is a pressing need for a decentralized secure architecture independent of RSUs and centralized systems.

VI. Security Analysis

This section presents informal and formal security analyzes to demonstrate the safety and security of the proposed system against various possible attacks

Raw security: A detailed informal safety analysis of the given protocol is presented as follows.

Correct assumptions about user anonymity: Unlike many authentication schemes for multi-server environments where the server cannot recognize the user making the login request, our protocol maintains a dynamic pseudo-identity (PIDu) when the authentication request goes to Sj Using the user's identity (IDu) only the server's private key Only can be removed, ensuring that the user is anonymous and traceable.

Repeated Attacks: In replay attacks, where an adversary intercepts messages to deceive legitimate users, our protocol ensures security by creating two unique challenge-responses (Cu and Dj) for each session so even if the enemy accepts parameters they cannot launch an attack.

Sneaky smart card attacks with offline dictionaries: Attempts by the adversary to guess a password (PWu) from known parameters (Yu and Fu) to mitigate smart card attacks stolen through the offline dictionary fail because the system configuration makes these attacks impossible in polynomial time using the smart card

Key Known Safety: The protocol provides known-key security by ensuring the confidentiality of the private key even if the session key is exposed, preventing adversaries from seeing the parameters from the derived session key

Mutual recognition: Our enhanced system ensures mutual recognition by legitimate stakeholders, enabling faster detection of potential attacks such as counterattacks.

Mask Attack: The protocol doesn’t cover masquerade attacks, because the stolen card doesn’t show important parameters like Xu, and prevents attackers from impersonating legitimate users

Verifier Stolen Attacks: Adversaries trying to exploit data stored on the server side or the user's privacy cannot pose as legitimate users, because the protocol provides mutual authentication without managing storage on the server-client side

Password guessing attacks: While password guessing attacks are possible if adversaries access certain criteria, the protocol reduces the chances of correctly guessing passwords because they are not used in the audit

Change Attacks: The protocol effectively resists modification attacks by ensuring that modifications to public information cannot be reassembled without knowledge of a private key, enabling legitimate members to quickly detect malicious activity

Formal security assessment: The security model for the given protocol is described in this section. Using this security measure, the protocol has been proven to be secure against known attacks. Moreover, the proposed protocol satisfies all important safety requirements.

VII. Existing Methodology

In the current environment, authentication and key compromise mechanisms in peer cloud systems exhibit diversity, often corresponding to exact applications and policies Below are some common mechanisms and technologies a an overview of their use in this area.

1. Public Key Infrastructure (PKI): This approach is based on a PKI architecture where peers obtain public and private key pairs from a trusted certificate authority (CA) Peers use their private keys for message sign and authentication , while secure communication channels are established over trusted CA certificates.
2. Anonymous authentication: Systems such as U-Prove and Idemix use anonymous certificate systems, which provide peer-to-peer authentication from trusted authorities that allow for authentication that does not reveal real identities. These certificates contain cryptographic evidence to ensure authenticity without revealing identity information.
3. Identity-Based Encryption (IBE): IBE schemes, such as Boneh-Franklin and Waters, enable secure communications by encrypting messages using the recipient’s identity as the public key and then their a they receive it using their private key derived from their identity to decrypt the message.
4. Group signatures:Group signatures systems enable peers to validate as members of the group without identifying individual identities. Peers sign messages using a group signature, allowing authentication without signer identification, facilitating trust and authentication in peer-to-peer cloud systems
5. Unsubstantiated knowledge: Unsubstantiated knowledge provides a way to prove a statement without disclosing additional information. Used in the indication and the main contract, these testimonials reveal hidden knowledge without revealing the secret itself, ensuring certification while maintaining anonymity

VIII. PROPOSED SYSTEM

Blockchain (BC) Existing research on relay vehicle selection mechanisms in Vehicular Ad-hoc Networks (VANETs) often fails in implementing complex multi-hop BC systems Several proposed mechanisms have been developed smart for one-hop or two-hop situations, including more complex multi -jumping. Employees do not have the power to use it effectively. Furthermore, these systems rely heavily on prearranged information, often based on GPS data, which can be unreliable, especially in urban areas with high-rise buildings
A recent study adds Road Side Units (RSUs) to their models, providing additional benefits. However, implementing RSUs in real-world situations is expensive and may not be feasible everywhere due to geographic limitations.

On the other hand, the proposed trust and special waiver agreement allows peer-to-peer cloud systems to offer a wide range of reward over existing systems:
1. Anonymity Protection: Prioritizes user anonymity, allowing authentication without revealing real identities, thus increasing privacy protection.
2. Decentralization and distribution of trust: It operates in a decentralized manner, thereby removing reliance on central authority and increasing system flexibility.
3. Enhanced Privacy Protection: Incorporates encryption, data anonymization, and secure communication channels to ensure sensitive user data remains private.
4. Scalability and efficiency: Designed to efficiently address scalability challenges, reduce overhead and ensure efficient use of resources.
5. Strong security measures: Perform strong security audits, integrate strong cryptography protocols to combat security threats.
6. Interoperability and Compatibility:Integrates seamlessly with existing systems and protocols, facilitating interoperability across platforms.
8. Improved user experience:Increases user satisfaction by prioritizing functionality through easy-to-use interfaces and simplified methods, while maintaining security and in private.

Taking advantage of these advantages, the proposed mechanism enhances the security, privacy, scalability, efficiency, and collaboration of the peer cloud system, and provides a robust approach to collaboration protection while preserving user anonymity and confidentiality

IX. System Design

UML DIAGRAM

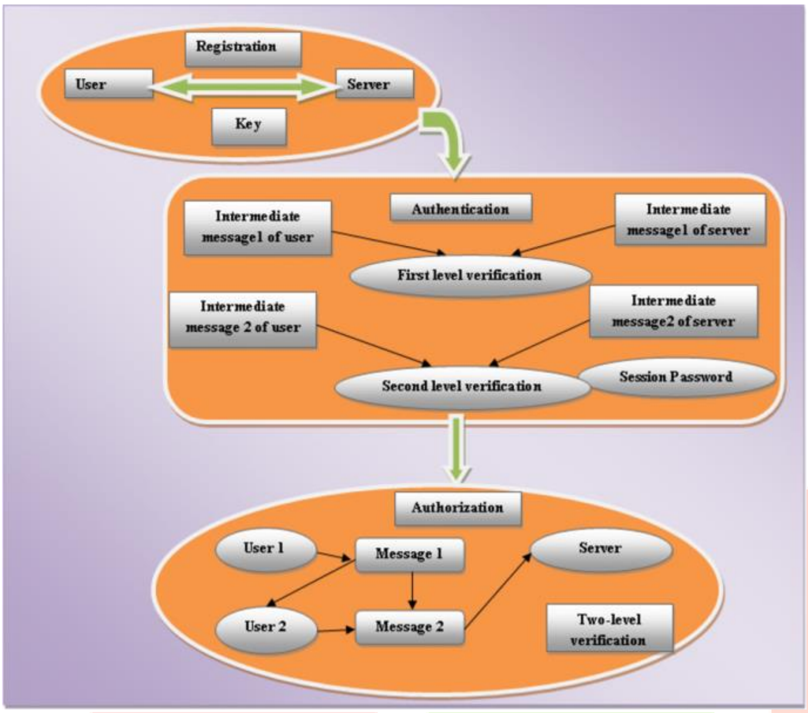


Figure 2 : UML of Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud

Use Case Diagram:

- Use case diagrams show how the system works from the user's perspective.
- It identifies various stakeholders (users, systems, or external agencies) and their interactions with the system.
- Use case diagrams show high-level system requirements and key tasks or activities performed by users.

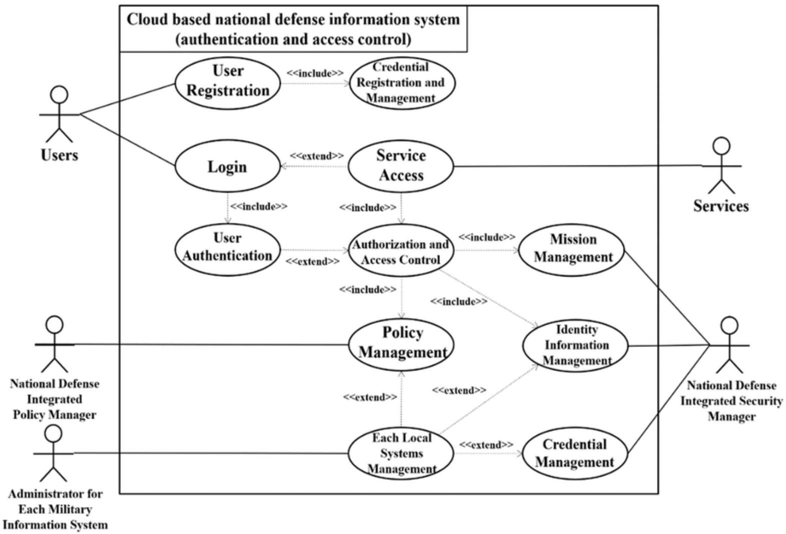
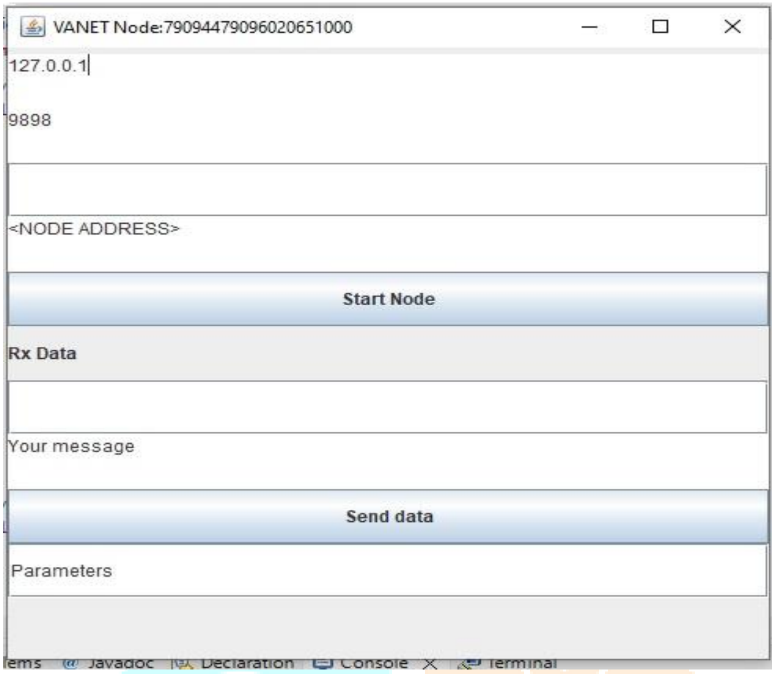

Cloud based national defense information system (authentication and access control)
Users
User Registration
<<include>>
Credential Registration and Management
Login
<<extend>>
Service Access
Services
<<include>>
<<include>>
User Authentication
<<extend>>
Authorization and Access Control
<<include>>
Mission Management
<<include>>
<<include>>
Policy Management
Identity Information Management
National Defense Integrated Policy Manager
<<extend>>
<<extend>>
National Defense Integrated Security Manager
Each Local Systems Management
<<extend>>
Credential Management
Administrator for Each Military Information System

Figure 3: Use Case Diagram of Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud

X. RESULT

Screen shots:



VANET Node:790944790960206510000

127.0.0.1

9898

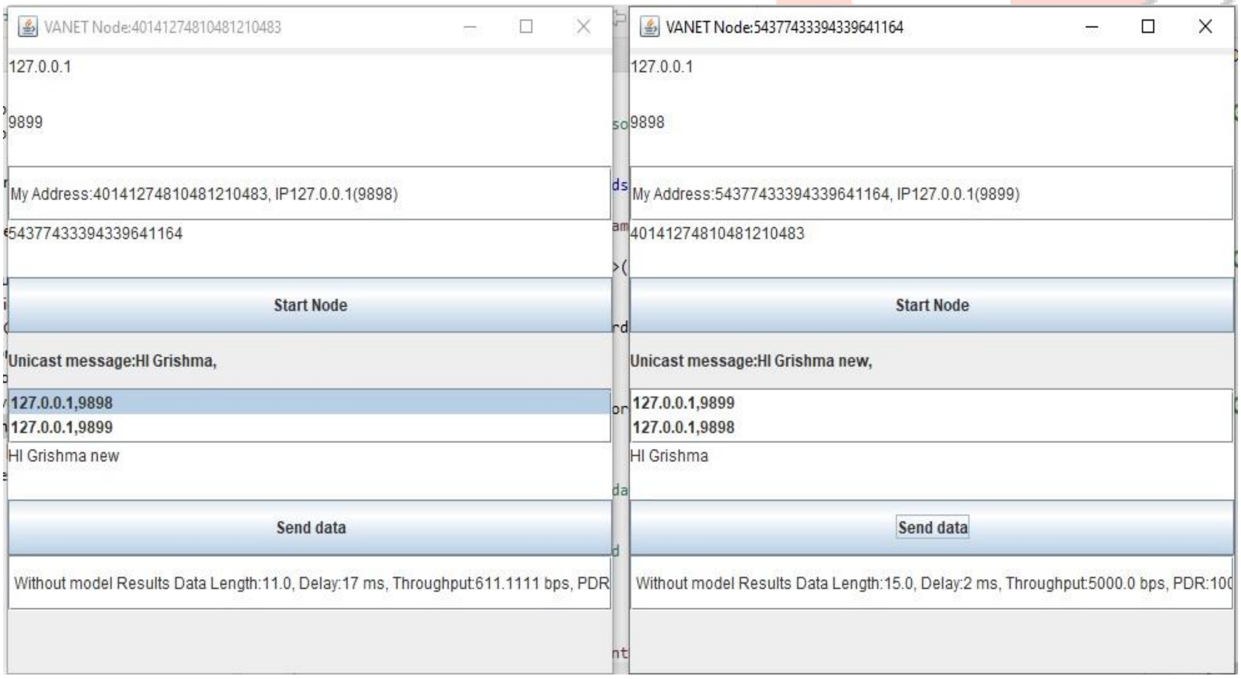
<NODE ADDRESS>

Rx Data

Your message

Parameters

Figure 4: Sender of Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud



VANET Node:40141274810481210483

127.0.0.1

9899

My Address:40141274810481210483, IP127.0.0.1(9898)

54377433394339641164

Unicast message:HI Grishma,

127.0.0.1,9898
127.0.0.1,9899

HI Grishma new

Without model Results Data Length:11.0, Delay:17 ms, Throughput:611.1111 bps, PDR

VANET Node:54377433394339641164

127.0.0.1

9898

My Address:54377433394339641164, IP127.0.0.1(9899)

40141274810481210483

Unicast message:HI Grishma new,

127.0.0.1,9899
127.0.0.1,9898

HI Grishma

Without model Results Data Length:15.0, Delay:2 ms, Throughput:5000.0 bps, PDR:10

Figure 5: Sender and Receiver Node of Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud

XI. CONCLUSION:

In summary, authentication and special contract mechanisms represent a key component in peer-to-peer cloud infrastructure, providing secure and anonymous communications between peers through strong security protocols, privacy protection mechanisms and cryptographic algorithms a strong inclusion, system security environment provides a space for users to be independent and establish secure communication channels The proposed system offers more advantages than solutions with already there, especially improved security, privacy protection, scalability, connectivity, and user friendliness
The proposed tool combines features such as anonymous authentication, secure key agreement protocol, and privacy enhancement technologies to overcome current system deficiencies Software requirements specification defines active and passive system requirements, while external interface requirements dictate interfaces with external systems Security, privacy, scalability , guided by system objectives and principles that prioritize implementation and compliance, are designed. UML diagrams act as visual aids, showing usability, class hierarchy, sequential actions, interconnected components, and hierarchy. These diagrams facilitate understanding of organizational structures, practices, and relationships, thereby improving communication, planning, and documentation processes. Following the design objectives, principles, and module specifications, the special authentication, and contracting mechanisms are poised to deliver a secure, privacy-protecting, scalable, and user-friendly solution peer cloud systems Confidentiality, integrity, and authenticity of user data and communications while maintaining privacy To ensure that the system provides seamless collaboration between peers

REFERENCES

1. Bogdan Alexe, Thomas Deselaers, and Vittorio Ferrari, “What is an object?”,
2. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2010.
3. 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“.
4. Design of a Convolutional Neural Network Based Smart Waste Disposal System.
5. Thung, Gary and M. Yang. “Classification of Trash for Recyclability Status.” (2016).
6. 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.
7. George E Sakr, Maria Mokbel, Ahmad Darwich, Mia Nasr Khneisser and Ali Hadi, “Comparing Deep Learning And Support Vector Machines for Autonomous Multidisciplinary Conference.
8. 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.
9. “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.
10. 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.
11. 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].
12. K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” in 2016 IEEE

13. Conference on Computer Vision and Pattern
14. Recognition (CVPR), Las Vegas, NV, USA, pp. 770–778, Jun. 2016. doi: 10.1109/CVPR.2016.90.
15. 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.
16. M. Yang and G. Thung, “Classification of Trash for Recyclability Status,” Stanford University, CS229, 2016.
17. 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, pp.1–7, Jul. 2018. doi: 10.1109/INISTA.2018.8466276.
18. H. Khan, “Transfer learning using mobilenet,” 2019. [Accessed Sep. 23, 2019].
19. Kochalko, D. Making the unconventional conventional: How blockchain contributes to reshaping scholarly communications. *Inf. Serv. Use* **2019**, *39*, 199–204. [CrossRef]
20. 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]
21. 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]
22. 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]
23. Tan, S.; Wang, X.; Jiang, C. Privacy-Preserving Energy Scheduling for ESCOs Based on Energy Blockchain Network. *Energies* **2019**, *12*, 1530. [CrossRef]
24. 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]
25. Ekstrom, S. Freud, Jung and The Great Chain of Being. *J. Anal. Psychol.* **2018**, *63*, 462–483. [CrossRef]
26. Raqui, Y. A Peer-to-Peer Ecosystem for Cash Equity Trading. *SSRN Electron. J.* **2019**. [CrossRef]
27. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
28. Khaqqi, K.N.; Sikorski, J.J.; Hadinoto, K.; Kraft, M. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Appl. Energy* **2018**, *209*, 8–19. [CrossRef]
29. Luo, X.; Xue, K.; Xu, J.; Sun, Q.; Zhang, Y. Blockchain Based Secure Data Aggregation and Distributed Power Dispatching for Microgrids. *IEEE Trans. Smart Grid* **2021**, *12*, 5268–5279. [CrossRef]
30. Yang, J.; Dai, J.; Gooi, H.B.; Nguyen, H.D.; Wang, P. Hierarchical Blockchain Design for Distributed Control and Energy Trading within Microgrids. *IEEE Trans. Smart Grid* **2022**, *13*, 3133–3144. [CrossRef]

31. Alonso, M.; Amaris, H.; Alcala, D.; Florez R., D.M. Smart Sensors for Smart Grid Reliability. *Sensors* **2020**, *20*, 2187. [CrossRef]

32. Kim, Y.; Hakak, S.; Ghorbani, A. Smart grid security: Attacks and defence techniques. *IET Smart Grid* **2022**. [CrossRef]

33. Chen, K.-L.; Yang, X.; Xu, W. Contactless Voltage Distortion Measurement Using Electric Field Sensors. *IEEE Trans. Smart Grid* **2018**, *9*, 5643–5652. [CrossRef]

34. Song, E.Y.; Fitz Patrick, G.J.; Lee, K.B.; Griffor, E. A Methodology for Modeling Interoperability of Smart Sensors in Smart Grids. *IEEE Trans. Smart Grid* **2022**, *13*, 555–563. [CrossRef]

35. Kerk, S.G.; Hassan, N.U.; Yuen, C. Smart Distribution Boards (Smart DB), Non-Intrusive Load Monitoring (NILM) for Load Device Appliance Signature Identification and Smart Sockets for Grid Demand Management. *Sensors* **2020**, *20*, 2900. [CrossRef] [PubMed]

36. Khan, M.A.; Hayes, B. PTP-based time synchronisation of smart meter data for state estimation in power distribution networks. *IET Smart Grid* **2020**, *3*, 705–712. [CrossRef]

37. Caterino, N.; Spizzuoco, M.; Occhiuzzi, A. Shaking table testing of a steel frame structure equipped with semi-active MR dampers: Comparison of control algorithms. *Smart Struct. Syst.* **2015**, *15*, 963–995. [CrossRef]

38. Rajalingam, S.; Malathi, V. HEM algorithm based smart controller for home power management system. *Energy Build.* **2016**, *131*, 184–192. [CrossRef]

39. Fan, W.; Liu, N.; Zhang, J. An Event-Triggered Online Energy Management Algorithm of Smart Home: Lyapunov Optimization Approach. *Energies* **2016**, *9*, 381. [CrossRef]

40. Sezer, V. Intelligent decision making for overtaking maneuver using mixed observable Markov decision process. *J. Intell. Transp. Syst.* **2017**, *22*, 201–217. [CrossRef]

41. Lizán, F.J.M. Intelligent Buildings: Foundation for Intelligent Physical Agents. *Int. J. Eng. Res. Appl.* **2017**, *7*, 21–25. [CrossRef]

42. Dai, R.; Liu, G.; Wang, Z.; Kan, B.; Yuan, C. A Novel Graph-Based Energy Management System. *IEEE Trans. Smart Grid* **2019**, *11*, 1845–1853. [CrossRef]

43. Chhaya, L.; Sharma, P.; Kumar, A.; Bhagwatikar, G. IoT-Based Implementation of Field Area Network Using Smart Grid Communication Infrastructure. *Smart Cities* **2018**, *1*, 176–189. [CrossRef]

44. Aleksic, S. A Survey on Optical Technologies for IoT, Smart Industry, and Smart Infrastructures. *J. Sens. Actuator Netw.* **2019**, *8*, 47. [CrossRef]

45. Yousif, M. Convergence of IoT, Edge and Cloud Computing for Smart Cities. *IEEE Cloud Comput.* **2018**, *5*, 4–5. [CrossRef]

46. Yaghmaee, M.H.; Leon-Garcia, A.; Moghaddassian, M.; Moghaddam, M.H.Y. On the Performance of Distributed and Cloud-Based Demand Response in Smart Grid. *IEEE Trans. Smart Grid* **2018**, *9*, 5403–5417. [CrossRef]

47. Rahmani, R.; Li, Y. A Scalable Digital Infrastructure for Sustainable Energy Grid Enabled by Distributed Ledger Technology.

J. Ubiquitous Syst. Pervasive Networks **2020**, *12*, 17–24. [CrossRef]

48. Almehizia, A.A.; Al-Masri, H.M.K.; Ehsani, M. Integration of Renewable Energy Sources by Load Shifting and Utilizing Value Storage. *IEEE Trans. Smart Grid* **2019**, *10*, 4974–4984. [CrossRef]

49. Donaldson, D.L.; Jayaweera, D. Effective solar prosumer identification using net smart meter data. *Int. J. Electr. Power Energy Syst.* **2020**, *118*, 105823. [CrossRef]

50. Schultis, D.-L.; Ilo, A.; Schirmer, C. Overall performance evaluation of reactive power control strategies in low voltage grids with high prosumer share. *Electr. Power Syst. Res.* **2019**, *168*, 336–349. [CrossRef]

51. Wesche, J.P.; Dütschke, E. Organisations as electricity agents: Identifying success factors to become a prosumer. *J. Clean. Prod.* **2021**, *315*, 127888. [CrossRef]

52. Shin, M.; Kim, H.; Kim, H.; Jang, H. Building an Interoperability Test System for Electric Vehicle Chargers Based on ISO/IEC 15118 and IEC 61850 Standards. *Appl. Sci.* **2016**, *6*, 165. [CrossRef]

53. Farooq, S.M.; Hussain, S.M.S.; Kiran, S.; Ustun, T.S. Certificate Based Authentication Mechanism for PMU Communication Networks Based on IEC 61850-90-5. *Electronics* **2018**, *7*, 370. [CrossRef]

54. Bao, K.; Valev, H.; Wagner, M.; Schmeck, H. A threat analysis of the vehicle-to-grid charging protocol ISO 15118. *Comput. Sci. Res. Dev.* **2017**, *33*, 3–12. [CrossRef]

55. Lee, S. Study on Electric Vehicles and Communication Technologies in Smart Grid Environment. *Int. J. Control. Autom.* **2018**, *11*, 163–170. [CrossRef]

56. Khazaei, J.; Nguyen, D.H. Multi-Agent Consensus Design for Heterogeneous Energy Storage Devices with Droop Control in Smart Grids. *IEEE Trans. Smart Grid* **2019**, *10*, 1395–1404. [CrossRef]

57. Kofinas, P.; Dounis, A.; Vouros, G. Fuzzy Q-Learning for multi-agent decentralized energy management in microgrids. *Appl. Energy* **2018**, *219*, 53–67. [CrossRef]

58. Miao, Z.; Fan, L. A Novel Multi-Agent Decision Making Architecture Based on Dual's Dual Problem Formulation. *IEEE Trans. Smart Grid* **2018**, *9*, 1150–1160. [CrossRef]

59. Alshahrani, M.; Traore, I. Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *J. Inf. Secur. Appl.* **2019**, *45*, 156–175. [CrossRef]

60. Sundararajan, A.; Hernandez, A.S.; Sarwat, A.I. Adapting big data standards, maturity models to smart grid distributed generation: Critical review. *IET Smart Grid* **2020**, *3*, 508–519. [CrossRef]

61. Treiblmaier, H. Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. *Front. Blockchain* **2019**, *2*, 3. [CrossRef]

62. Hang, L.; Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* **2019**, *19*, 2228. [CrossRef] [PubMed]

63. Garlapati, S. Blockchain for IOT-based NANs and HANs in Smart Grid. *SSRN Electron. J.* **2020**. [CrossRef]

64. Zhang, Y.; Yau, D.; Zonouz, S.; Jin, N.; Qiu, M.; Erol-Kantarci, M. Guest Editorial Smart Grid Cyber-Physical Security. *IEEE Trans. Smart Grid* **2017**, *8*, 2409–2410. [CrossRef]

65. Diestelmeier, L. Changing power: Shifting the role of electricity consumers with blockchain technology—Policy implications for EU electricity law. *Energy Policy* **2019**, *128*, 189–196. [CrossRef]