

Stealth Voice Communication System Using Blockchain-Based Identity Verification

SHAIK MUBASHEER (U22CN257)

S.I CHIDVILAS (U22CN228)

SHUBHAM KUMAR (U22CN282)

SIDHARTH KUMAR (U22CN283)

Under the guidance of

Mrs. K. Sathiya Priya M. Tech., Ph. D

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

BHARATH INSTITUTE OF SCIENCE AND TECHNOLOGY

BHARATH INSTITUTE OF HIGHER EDUCATION AND RESEARCH

(Deemed to be University Estd u/s 3 of UGC Act, 1956)

ABSTRACT

The Stealth Voice Communication System with Blockchain-Based One-Time Token is a secure communication framework designed to enable private voice communication between users. The system follows a layered architecture consisting of a Client Layer, Application Server, Blockchain Layer, and Communication Layer. A one-time token is generated and verified through blockchain smart contracts to ensure secure authentication and prevent unauthorized access. After successful verification, a peer-to-peer voice connection is established using WebRTC with encrypted communication. This approach improves privacy, security, and reliability in voice communication systems.

Stealth Voice Communication System Using Blockchain-Based Identity Verification is a secure communication framework designed to protect user identity and ensure trustworthy voice-based interaction. The project focuses on creating a communication environment where users can exchange voice messages or conduct voice communication without revealing sensitive identity details to unauthorized parties. By integrating blockchain-based identity

verification, the system adds an additional layer of trust, authenticity, and security to the communication process.

The proposed system uses blockchain technology to store and verify identity credentials in a decentralized and tamper-resistant manner. This helps prevent impersonation, unauthorized access, and identity fraud. At the same time, the voice communication module ensures private and efficient communication between verified users. The system is designed to be lightweight, secure, and suitable for applications where confidentiality and identity protection are important. Overall, the project presents a modern approach to secure communication by combining privacy, authentication, and decentralized verification in a single solution.

The main idea of the project is to ensure that only verified users can access and participate in the voice communication process. Blockchain is used to store and validate identity information in a decentralized manner, which makes the verification process highly secure and resistant to tampering. Unlike traditional centralized systems, blockchain reduces the risk of identity theft and unauthorized modification of records. At the same time, the stealth voice communication module helps hide or protect sensitive user information while allowing secure voice exchange between authenticated users. This makes the system suitable for applications where confidentiality, anonymity, and trust are essential.

CHAPTER 1

INTRODUCTION

Stealth Voice Communication System Using Blockchain-Based Identity Verification is a secure communication project designed to protect user identity and improve trust during voice communication. The main goal of this system is to allow authorized users to communicate safely while preventing identity fraud, unauthorized access, and misuse of voice data. By combining stealth communication techniques with blockchain-based authentication, the project offers a modern and reliable approach to privacy-focused communication.

In traditional communication systems, user information is often stored in centralized servers, which can be vulnerable to hacking, data tampering, and impersonation attacks. This project addresses those issues by introducing a decentralized verification mechanism based on blockchain technology. Since blockchain records are distributed, immutable, and difficult to

alter, it provides a stronger level of trust for identity verification. The system verifies each user before allowing communication, ensuring that only authenticated participants can access the platform.

The stealth voice communication feature adds another layer of privacy by reducing the exposure of sensitive communication details. This is especially useful in applications where confidentiality is essential, such as corporate communication, defense, healthcare, and private messaging. The project aims to create a system that is not only secure but also practical and user-friendly. It focuses on maintaining a balance between privacy, authentication, and ease of use so that users can communicate confidently without worrying about identity misuse.

Overall, the project demonstrates how blockchain can be integrated with voice communication to build a more secure and trustworthy platform. It supports the idea of decentralized identity management while ensuring that voice communication remains private and protected. This makes the system a valuable solution for modern communication environments where security and anonymity are increasingly important.

1.1 Overview

The project Stealth Voice Communication System Using Blockchain-Based Identity Verification focuses on building a secure and private voice communication platform. Its main purpose is to allow only verified users to communicate while protecting identity, preventing unauthorized access, and reducing the risk of impersonation or data misuse.

The system combines two important ideas. First, blockchain-based identity verification is used to confirm user authenticity in a decentralized and tamper-resistant way. Second, stealth voice communication is used to keep the communication process private and reduce exposure of sensitive information. Together, these features create a more trustworthy communication environment.

The system combines blockchain-based authentication with stealth communication techniques. Blockchain helps verify users in a secure and tamper-resistant manner, while stealth

communication protects the transmitted voice data from exposure. By integrating these two approaches, the proposed model creates a communication environment that is safer, more trustworthy, and better suited for confidential exchanges.

This project is useful in situations where confidentiality is very important, such as defense communication, corporate messaging, healthcare discussions, and secure personal communication. It aims to provide a solution that is not only secure but also practical, reliable, and easy to use.

Overall, the project addresses the growing need for safer communication systems in the digital era. It demonstrates how blockchain technology can be applied beyond finance to improve privacy, identity security, and trust in voice communication platforms.

This overview introduces the central idea of the project and explains the importance of secure communication in modern applications. It also prepares the reader for the later sections, where the background, objectives, implementation, and results are discussed in detail.



1.1 System Architecture

1.2 Background of the Project

In modern communication systems, privacy and identity protection have become very important concerns. Voice communication is widely used in personal, business, and

confidential environments, but traditional systems often rely on centralized servers and basic authentication methods. These approaches can be vulnerable to hacking, impersonation, and unauthorized access, which may compromise sensitive information and user trust.

Secure communication has become a major requirement in modern digital systems because users regularly exchange sensitive information through online platforms. Traditional communication methods often face problems such as unauthorized access, identity misuse, message interception, and privacy leakage. Because of these issues, there is a growing need for a communication framework that can provide both strong authentication and confidentiality.

Blockchain technology has emerged as a strong solution for improving trust in digital systems. Its decentralized and tamper-resistant nature makes it useful for identity verification and secure record management. In communication systems, blockchain can link user identities to public keys and help verify that messages or requests come from legitimate users, reducing the risk of impersonation and fraud.

At the same time, privacy-preserving communication methods are becoming increasingly important, especially for applications involving voice or confidential data exchange. A secure communication system should not only verify users but also protect the content being transmitted from unauthorized viewing or interception. This project addresses that need by combining blockchain-based verification with stealth communication techniques to create a more secure and trustworthy voice communication model.

The background of this project is based on the idea that secure communication should include both identity protection and data confidentiality. Blockchain helps ensure that only authenticated users can access the system, while stealth communication helps keep the transmitted voice data private. Together, these technologies form the foundation for a secure voice communication platform that is suitable for environments where trust, privacy, and reliability are essential.

To address these issues, this project introduces a secure communication framework that combines stealth voice communication with blockchain-based identity verification. Blockchain technology is known for its decentralized structure, tamper resistance, and transparency, making it suitable for verifying user identities without depending on a single central authority. This helps improve trust and reduces the risk of identity misuse or data alteration.

The project is especially relevant in fields where confidentiality is critical, such as defense, corporate communication, healthcare, and secure messaging platforms. By integrating privacy-focused voice communication with decentralized identity management, the system aims to provide a stronger and more reliable method of communication. This background forms the foundation for developing a secure, trustworthy, and modern voice communication solution.

In recent years, digital communication has become a major part of everyday life, and voice communication is one of the most commonly used methods for exchanging information. However, as communication grows more digital, the risk of privacy breaches, identity theft, and unauthorized access also increases. Many existing systems depend on centralized servers or simple login methods, which may not be strong enough to protect users from attacks or misuse. This creates a serious need for a more secure and trustworthy communication model.

At the same time, stealth voice communication adds an extra layer of privacy by minimizing the exposure of sensitive voice data. This is useful in situations where users need to communicate without revealing unnecessary personal details. The combination of stealth communication and blockchain-based verification creates a system that is both secure and privacy-oriented. It is especially suitable for environments where confidentiality is critical, such as military communication, corporate discussions, healthcare coordination, and secure personal messaging.

To solve these problems, modern systems are increasingly using blockchain technology because of its decentralized, transparent, and tamper-resistant nature. Blockchain can be used to verify identities and store trusted records without depending on a single central authority. This makes it highly useful in applications where authentication and data integrity are critical. In secure communication, blockchain helps ensure that only legitimate users can access the system and that records cannot be easily altered.

In recent years, secure communication has become an essential requirement in digital systems because a large amount of sensitive information is exchanged through online platforms. Users depend on communication systems for personal, academic, financial, and organizational purposes, so protecting that information from unauthorized access is very important. However, many traditional communication methods still face issues such as identity spoofing, message interception, data leakage, and lack of trust in user authentication.

The background of this project is based on the need for a communication system that is not only secure but also privacy-preserving and reliable. The proposed model addresses this need by integrating blockchain-based verification with stealth communication techniques. This combination is intended to improve trust, reduce unauthorized access, and ensure confidential voice communication in environments where security is highly important

This project is built on the idea that communication should not only be fast and convenient, but also secure and trustworthy. By integrating modern technologies, it aims to solve the limitations of traditional systems and provide a stronger framework for safe voice communication.

1.3 Problem Statement

In existing voice communication systems, user identity and communication privacy are not always fully protected. Many platforms depend on centralized authentication methods, which can be vulnerable to impersonation, unauthorized access, data tampering, and identity misuse. As a result, users may not have complete confidence that their communication is secure or that the person on the other end is genuinely authenticated.

There is therefore a need for a secure voice communication system that can verify user identity in a decentralized and tamper-resistant manner while also protecting privacy during communication. The challenge is to design a system that combines stealth voice communication with blockchain-based identity verification so that only legitimate users can communicate safely, confidentially, and reliably.

Modern voice communication systems are widely used for personal and professional interaction, but many of them still depend on centralized authentication and conventional login mechanisms. In such systems, user identities are often linked to phone numbers, usernames, or server-managed accounts, which can expose sensitive information and reduce privacy. As a result, the communication process becomes vulnerable to unauthorized access, identity leakage, and misuse of user data.

Another major issue in existing communication platforms is the lack of strong protection against impersonation and replay attacks. If an attacker obtains credentials or intercepts communication metadata, they may attempt to reuse access information or fake a legitimate user identity. Traditional verification methods are often not sufficient to stop such threats,

especially when the system relies on a single central authority for authentication and session control.

In addition, most existing systems do not provide a truly anonymous communication environment. Even when encryption is used for transmission, the identity of the participants may still be exposed through registration details, account information, or network traces. This creates a gap between secure transmission and secure identity management. Therefore, there is a need for a voice communication model that protects both the content of the call and the identity of the users involved.

To address these issues, a more secure and privacy-focused approach is required. The proposed system aims to combine blockchain-based one-time token verification with encrypted peer-to-peer voice communication, so that only authorized users can connect while personal identity remains hidden. This approach is intended to improve authentication strength, prevent unauthorized access, and provide a more reliable framework for stealth voice communication.

In present-day communication systems, voice interaction is widely used for personal, business, and confidential purposes. However, many existing platforms do not provide strong enough protection for user identity and communication privacy. Most of these systems depend on centralized authentication methods, which can be easily targeted by attackers. This may lead to problems such as impersonation, unauthorized access, interception of voice data, and misuse of sensitive information.

Another major issue is that traditional systems often lack a reliable mechanism to verify whether a user is genuine or not. Even if a communication channel is active, there is no guarantee that the participant on the other end is an authorized person. This creates a trust problem and reduces the overall security of the communication process. In addition, many systems expose more user information than necessary, which can compromise privacy.

Therefore, there is a clear need for a secure voice communication system that ensures both privacy and identity verification. The proposed solution should make use of blockchain technology to store and verify identity information in a decentralized and tamper-resistant way. At the same time, it should support stealth communication so that sensitive voice exchanges

remain protected from unauthorized access and exposure. The main problem addressed by this project is how to create a communication system that is secure, private, trustworthy, and suitable for real-world use.

1.4 Objectives of the Project

The main objective of this project is to develop a secure and privacy-focused voice communication system that protects user identity during communication. The project aims to ensure that only authenticated users can access the communication platform and exchange voice messages safely.

The specific objectives of the project are:

- design a stealth voice communication system that minimizes exposure of sensitive information.
- To use blockchain technology for secure and decentralized identity verification.
- To prevent unauthorized access, impersonation, and identity fraud.
- To maintain confidentiality and trust during voice communication.
- To build a system that is efficient, reliable, and suitable for real-world applications.
- To provide a user-friendly platform that combines privacy with strong security.

The main objective of this project is to develop a secure and privacy-focused voice communication system that protects user identity during communication. The system is intended to allow only authorized users to communicate, ensuring that voice exchanges remain confidential, trustworthy, and resistant to unauthorized access.

The project also aims to combine stealth communication with blockchain-based identity verification so that the communication process becomes more secure and reliable. Blockchain is used because it provides decentralized and tamper-resistant identity management, which helps prevent impersonation, fake accounts, and modification of user records. This makes the system more dependable than traditional centralized communication methods.

The project has the following specific objectives:

- To implement a secure authentication mechanism using blockchain technology.

- To ensure that only authorized users can access the communication system.
- To protect voice communication from unauthorized monitoring or interception.
- To improve trust and transparency in the verification process.
- To provide a privacy-preserving communication method for sensitive information exchange.
- To build a practical system that can be used in real-world secure communication scenarios.

Another important objective is to demonstrate how blockchain can be integrated with communication security techniques to improve overall system performance. The project also aims to reduce the risks commonly found in traditional communication systems by adding a tamper-resistant verification layer. In this way, the system becomes more suitable for environments where confidentiality and reliability are essential.

1.5 Summary

This project focuses on building a secure voice communication system that protects user identity and improves privacy during communication. It uses blockchain-based identity verification to ensure that only authenticated users can access the system, reducing the risk of impersonation, unauthorized access, and identity fraud. The stealth communication feature adds an extra layer of confidentiality by keeping sensitive communication details protected.

Overall, the project combines privacy, trust, and security in a single framework. It is designed to be practical, reliable, and suitable for real-world applications where secure communication is important.

This project presents a secure and privacy-oriented voice communication solution that is designed to protect both user identity and communication content. In today's digital environment, voice communication is often exposed to risks such as impersonation, unauthorized access, and misuse of personal information. To address these issues, the proposed system combines stealth communication techniques with blockchain-based identity verification, creating a safer and more trustworthy communication platform.

The system ensures that only verified users can participate in communication by using blockchain as a decentralized and tamper-resistant method of authentication. This reduces

dependence on traditional centralized servers and lowers the chances of identity fraud or data manipulation. At the same time, the stealth communication feature helps keep sensitive communication details hidden from unauthorized users, improving confidentiality.

The project is useful in applications where security and privacy are highly important, such as military communication, corporate environments, healthcare systems, and private messaging platforms. By integrating authentication, privacy, and secure communication into one framework, the project offers a modern solution to the limitations of traditional voice communication systems.

This chapter introduced the basic concept of the project and explained why secure voice communication is important in modern digital systems. It described the need for a system that can protect user identity, prevent unauthorized access, and maintain the confidentiality of voice data. The background of the project showed that traditional communication methods often face security and privacy issues, which makes a stronger solution necessary.

The chapter also presented the main objectives of the project, which are to use blockchain-based verification and stealth communication to improve security and privacy.

CHAPTER 2

LITERATURE SURVEY

The literature survey reviews the existing work related to secure voice communication and identity verification. It helps identify the limitations of current approaches and shows why a more secure solution is needed for the proposed system. In many existing systems, communication security depends on centralized authentication, which can be vulnerable to attacks, impersonation, and unauthorized access. These weaknesses make it difficult to ensure both privacy and trust in voice-based communication.

A number of studies have focused on improving communication security through encryption, user authentication, and access control. While these methods provide a certain level of protection, they often depend on a central authority or a single point of control. If that authority is compromised, the entire system may become insecure. This limitation has encouraged researchers to explore decentralized technologies that can provide stronger and more reliable security.

Blockchain technology has emerged as one of the most promising solutions for identity verification and secure data management. It offers decentralized storage, immutability, and transparency, which make it difficult for attackers to tamper with identity records. Several research works have shown that blockchain can improve trust in systems where user authentication is critical. Because of these advantages, blockchain is increasingly being considered for secure communication applications.

At the same time, privacy-focused communication techniques are being developed to protect the content and details of communication from unauthorized users. Stealth communication methods aim to hide or minimize sensitive information so that only intended users can access it. However, many of these approaches do not fully solve the identity verification problem. As a result, there is still a gap between privacy protection and trustworthy authentication.

This project addresses that gap by combining stealth voice communication with blockchain-based identity verification. The literature suggests that a system integrating both privacy and secure authentication would be more effective than methods that focus on only one aspect. Therefore, the proposed work builds on existing research while improving the overall security, trust, and confidentiality of voice communication.

2.1 Existing Communication Systems

Existing communication systems are designed mainly to support fast and convenient voice or data exchange between users. However, many of these systems rely on centralized servers, basic login credentials, and standard network protections, which can leave them vulnerable to interception, spoofing, eavesdropping, and unauthorized access. In voice-based systems, security is even more challenging because attackers can exploit weaknesses in speaker verification and use synthetic or cloned voices to impersonate legitimate user.

Most traditional systems also do not provide strong built-in identity assurance. If passwords, tokens, or user records are compromised, attackers may gain access to communication channels without being detected. Research on communication security highlights that open or weakly protected networks can be exposed to man-in-the-middle attacks, replay attacks, packet manipulation, and privacy breaches. These limitations show that existing communication platforms often protect connectivity, but not always identity integrity and confidential voice exchange at the level required for sensitive applications.

Table 2.1

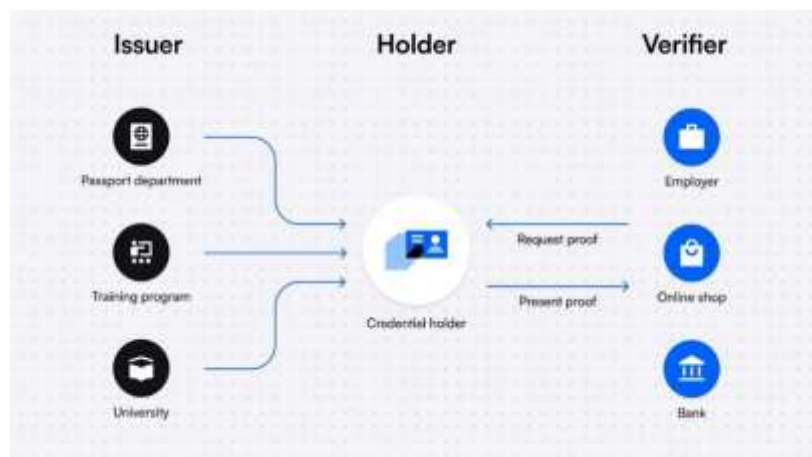
S. No.	Area	Description	Limitation
1	Voice Communication Systems	Used for fast and convenient communication between users.	Often vulnerable to interception and unauthorized access.
2	Centralized Authentication	Uses usernames, passwords, or server-based login methods.	If credentials are stolen, access can be easily misused.
3	Voice Authentication	Verifies users based on voice features.	Can be attacked using spoofing, cloning, or synthetic voice.
4	Network Security	Protects communication channels using standard encryption and controls.	May still be exposed to replay, man-in-the-middle, or packet attacks.
5	Privacy Protection	Aims to keep communication confidential.	Does not always guarantee strong identity verification.

2.1 Limitations of Existing Identity Verification and Voice Communication Approaches

2.2 Blockchain-Based Security

Blockchain-based security is used to make identity verification and communication more trustworthy by removing dependence on a single central authority. In secure voice communication, this is important because traditional key distribution and authentication methods can suffer from single points of failure, privacy issues, and weak trust management. By storing identity records and public keys on a decentralized ledger, blockchain helps make the verification process more transparent, tamper-resistant, and fault tolerant.

Research on blockchain-based VoIP systems shows that decentralized authentication can improve secure communication by allowing endpoints to verify each other before voice data is transmitted. Other work also notes that blockchain can eliminate the need for traditional certificate authorities, while still supporting key retrieval and end-to-end encryption for voice packets. This makes blockchain a strong fit for systems that need both identity assurance and privacy protection.



Issuer-Holder-Verifier model

Table 2.2

S. No.	Area	Description	Benefit
1	Decentralized Authentication	Identity verification is done through blockchain instead of a central server.	Reduces single points of failure and improves trust.
2	Public Key Management	User public keys can be stored and retrieved from the ledger.	Eliminates dependence on certificate authorities.
3	Tamper Resistance	Blockchain records are difficult to modify without detection.	Protects identity data from unauthorized changes.

S. No.	Area	Description	Benefit
4	Transparency	Verification steps can be traced on the ledger.	Improves account.ability and auditability.
5	Secure Voice Communication	Blockchain can support secure VoIP and call setup.	Helps ensure only verified users communicate.

2.2 Benefits of Blockchain-Based Authentication in Secure Voice Communication

Blockchain-based security plays an important role in making the voice communication system more reliable and trustworthy. In traditional systems, identity verification often depends on a central server or a third-party authority. If that server is attacked, compromised, or altered, the entire authentication process may become unsafe. Blockchain solves this problem by distributing the identity information across multiple nodes, which makes unauthorized modification much more difficult.

Another important advantage of blockchain is immutability. Once identity-related information is added to the blockchain, it cannot be changed easily without leaving evidence. This helps prevent tampering, impersonation, and fake identity creation. In a secure voice communication system, this is very useful because it ensures that only genuine users can participate in the communication process.

2.3 Identity Verification Approaches

Identity verification in communication systems is the process of confirming that a user is genuine before granting access. Common approaches include knowledge-based verification, biometric authentication, two-factor authentication, database-based verification, and online identity checks.

Knowledge-based verification depends on information only the user is expected to know, while biometric methods use unique physical traits such as fingerprints or facial features. Two-factor authentication improves security by combining something the user knows with something they possess, making unauthorized access harder.

Identity verification approaches are the methods used to confirm that a user is authentic before access is granted to a system or service. In secure communication applications, this step is especially important because it prevents unauthorized users from entering the network, impersonating someone else, or misusing private services. A weak verification process can expose the entire system to fraud, replay attacks, and privacy breaches.

The most common approach is knowledge-based verification, which relies on information that only the real user is supposed to know. This includes passwords, PINs, security questions, or secret codes. Although this method is easy to implement and widely used, it has a major limitation: the secret can be guessed, stolen, shared, or leaked through phishing or poor user behavior. Because of this, knowledge-based methods alone are no longer considered strong enough for high-security applications.

Another important approach is biometric authentication. This method verifies identity using physical or behavioral features such as fingerprints, face patterns, iris structure, voice characteristics, or typing rhythm. Biometrics are harder to copy than passwords, which makes them more secure in many cases. However, they also require specialized hardware or software, and they may create privacy concerns because biometric data is sensitive and cannot be changed once compromised.

A more secure method is two-factor authentication, where the system asks for two separate forms of proof before granting access. For example, a user may enter a password and then confirm a one-time code sent to a phone or email. This approach is stronger than password-only authentication because even if one factor is stolen, the attacker still needs the second factor. However, the security still depends on how safely the second factor is delivered and stored.

Database-based verification is also widely used in centralized systems. In this method, the system compares the submitted identity information with records stored in a trusted database. It is useful in organizational environments where user profiles, access rights, and login credentials are maintained in one place. The drawback is that if the database itself is attacked or corrupted, all stored identities may become vulnerable at once.

Online identity verification is another modern technique used in remote systems. It may involve checking email addresses, mobile numbers, digital documents, or government-issued IDs

through external verification services. This method is especially useful for systems that operate online and need to validate a user without physical presence. At the same time, it often depends on third-party services, which may reduce control and introduce extra trust requirements.

In the context of secure voice communication, identity verification must do more than just confirm login details. It should ensure that the correct user is allowed to establish a call while keeping personal identity hidden from outsiders. For this reason, traditional methods alone are not always suitable for privacy-focused applications. A stronger model, such as blockchain-based token verification, can provide authentication without exposing private user information directly.

Identity verification is one of the most important parts of any secure communication system. It is the process of confirming that a user is genuine before the system allows access to protected resources or communication features. In traditional applications, verification usually happens during login or registration, but in secure voice communication systems, it plays a much deeper role. It must ensure that the correct person is allowed to create or join a call while also protecting privacy and preventing unauthorized access.

The simplest and most common verification approach is knowledge-based verification. In this method, the system checks something the user knows, such as a password, PIN, passphrase, or security answer. This approach is easy to implement and familiar to users, which is why it is still widely used. However, it has many weaknesses. Users often choose weak passwords, reuse the same password across multiple services, or share their credentials accidentally. Passwords may also be stolen through phishing attacks, malware, or database leaks. Because of these risks, knowledge-based verification is not strong enough by itself for highly secure systems.

Another major approach is biometric authentication. Biometrics use unique physical or behavioral characteristics to identify a user. Examples include fingerprints, facial recognition, iris scanning, voice recognition, and even typing patterns. This method is more secure than password-only systems because biometric traits are difficult to copy or guess. It also improves convenience since users do not need to remember complex credentials. However, biometrics are not perfect. They may require special sensors, may fail under poor environmental conditions, and may raise privacy concerns because biometric data is sensitive and permanent. If biometric data is stolen, it cannot be changed like a password.

Two-factor authentication is another widely used method that provides a stronger level of security. In this approach, the user must prove identity using two different factors, usually something they know and something they possess. For example, a user may enter a password and then confirm a one-time password sent to a phone or email. This makes unauthorized access much harder because an attacker would need both factors. Even if one factor is compromised, the second layer still protects the account. Because of this, two-factor authentication is considered a major improvement over single-step login systems.

Database-based verification is commonly used in centralized systems. Here, the system checks the user's identity against stored records in a trusted database. This can include username-password pairs, registered mobile numbers, email addresses, or account IDs. Such systems are useful because they are easy to manage and can support large numbers of users. However, they also depend heavily on the security of the central database. If the database is attacked, corrupted, or leaked, a large amount of identity information may be exposed at once. This is one reason why centralized identity systems are often considered less secure for privacy-sensitive applications.

In secure voice communication systems, identity verification must balance three things: security, privacy, and usability. If the system is too weak, unauthorized users may enter the network, impersonate others, or misuse communication channels. If it is too strict, it may become difficult for legitimate users to access the service. For this reason, modern systems often combine multiple verification techniques instead of depending on only one method. This layered approach provides better protection and improves reliability.

In the proposed project, identity verification is handled in a more privacy-preserving way by using blockchain-based token validation. Instead of exposing the user's personal identity directly, the system verifies authorization through a one-time token stored and checked through smart contracts. This reduces the need for centralized identity storage and lowers the risk of impersonation. It also helps prevent replay attacks because the token can be used only once. As a result, the system supports secure authentication while preserving anonymity, which is very important in stealth voice communication.

Key Points to Include

- Identity verification ensures that only legitimate users can access the communication system.
- Password-based methods are simple but weak against modern attacks.
- Biometric methods are more secure but may create privacy and hardware issues.
- Two-factor authentication provides better protection than single-factor methods.
- Centralized database verification can be risky if the server is compromised.
- Blockchain-based token verification is suitable for anonymous and secure communication.

2.4 Stealth and Privacy-Oriented Communication

Stealth and privacy-oriented communication is focused on keeping voice exchange confidential while also reducing the ability of outsiders to detect, trace, or analyze the communication. In secure systems, privacy is not only about hiding the voice content, but also about protecting who is speaking, when communication happens, and how the data is transmitted. This is especially important in sensitive environments where even small leaks of information can create security risks.

A stealth communication approach usually combines several privacy techniques such as encryption, anonymization, and metadata reduction. Encryption protects the actual voice data so that unauthorized users cannot listen to it. Anonymization helps hide the identity of the speaker, while metadata reduction limits exposure of details like call time, **source**, destination, and traffic patterns. These measures work together to make the communication harder to intercept or interpret.

In a secure voice system, privacy-oriented communication also means that the user should control what information is shared and with whom. The system should avoid revealing unnecessary personal details and should ensure that communication remains accessible only to verified participants. This helps maintain confidentiality in applications such as defense, healthcare, corporate messaging, and private communication.

Another important point is that stealth communication must still remain practical and easy to use. A highly secure system is not useful if it is too difficult for users to adopt. For that reason, the proposed project aims to balance privacy, security, and usability. By combining stealth

communication with identity verification, the system can provide a safe communication channel without sacrificing convenience.

A common technique is **encryption**, which prevents unauthorized users from understanding transmitted voice data. Another important technique is **packet masking or tunneling**, where real communication is hidden inside other traffic so it becomes harder to detect or analyze. In addition, **voice anonymization** can transform speech so that speaker identity is concealed while keeping the spoken content usable, which is useful when privacy is more important than preserving the original voice characteristics

Stealth and privacy-oriented communication is designed to protect voice exchange in two ways: by securing the content of the message and by hiding the communication pattern itself. This matters because in many systems, attackers can learn useful information even if they cannot decrypt the audio, simply by observing who is communicating, when calls happen, or how traffic is routed. For a secure voice project, privacy must therefore cover both the speech and the surrounding communication metadata.

For this project, stealth communication is important because blockchain-based identity verification secures *who* is allowed to communicate, while privacy-oriented transmission secures *how* the communication takes place. Together, they reduce the risk of identity exposure, voice spoofing, and unwanted monitoring. This makes the system more suitable for confidential environments where trust and secrecy are both required.

2.5 Summary

In summary, identity verification is a key part of secure communication because it confirms that the right user is allowed to access the system. It helps protect the service from unauthorized access, impersonation, and misuse of private communication channels.

The common verification methods include passwords, biometrics, two-factor authentication, and database-based checks. Each of these methods improves security in its own way, but none of them is completely free from limitations. Passwords may be weak or stolen, biometric data may create privacy concerns, and centralized verification systems may be vulnerable if the stored data is exposed.

For a secure voice communication system, identity verification must also support anonymity and privacy. This means the system should validate users without revealing their personal identity unnecessarily. A blockchain-based one-time token approach is more suitable in this context because it provides tamper-resistant verification and reduces the risk of replay attacks.

Overall, the proposed approach is more secure and privacy-focused than traditional identity verification methods. It offers a practical way to combine authentication, anonymity, and secure access in a voice communication environment.

Stealth and privacy-oriented communication focus on making voice exchange both secure and difficult to trace. In this project, it helps ensure that voice data stays confidential while also reducing the exposure of user identity, call details, and communication patterns. This is important because protecting the content alone is not enough; the communication process itself must also remain private.

CHAPTER 3

PROPOSED METHODOLOGY

The proposed methodology explains how the Stealth Voice Communication System Using Blockchain-Based Identity Verification is designed and implemented. It describes the step-by-step process used to verify users, protect identity, and enable secure voice communication. The main aim of the methodology is to combine decentralized authentication with privacy-focused communication so that the system becomes both secure and practical.

This approach begins with user registration and identity verification, where blockchain is used to store and validate trusted identity information. After verification, the system creates a secure communication environment in which only authorized users can exchange voice data. At the same time, stealth communication techniques are applied to hide sensitive details and reduce the risk of interception or tracking.

The methodology is structured to ensure confidentiality, authenticity, and ease of use. Each stage of the process contributes to improving security and user trust while maintaining smooth communication. By integrating blockchain with stealth voice transmission, the proposed

system offers a modern solution for private and reliable communication in sensitive environments.

The methodology is built around three main goals: authentication, privacy, and secure delivery. First, the user is identified and verified through a blockchain-supported process that stores trusted identity records in a decentralized and tamper-resistant manner. Second, the system establishes a secure communication path that hides sensitive voice data and reduces exposure of user details. Third, the verified voice session is delivered only to authorized participants, ensuring confidentiality throughout the exchange.

This approach is important because traditional communication systems often depend on centralized servers and weak verification methods, which can create security and privacy risks. By using blockchain, the system removes single points of failure and improves trust. By using stealth communication techniques, it also protects the voice stream from unnecessary exposure. Together, these steps create a practical and modern framework for secure communication in sensitive environments.

31. System Design

The system design of **Stealth Voice Communication System Using Blockchain-Based Identity Verification** describes how the different parts of the project work together to provide secure and private communication. The design is centered on two main goals: verifying the identity of users through blockchain and protecting the voice communication through stealth and privacy-oriented methods. Each component is arranged to support secure access, confidential data transfer, and reliable communication.

The proposed system is designed as a secure and privacy-preserving voice communication platform that combines blockchain-based authentication with encrypted real-time communication. Its main purpose is to verify users without revealing unnecessary personal identity details and to ensure that only authorized users can establish a voice session. The design focuses on reducing trust in centralized control while improving security, transparency, and resistance to unauthorized access.

The system follows a layered architecture so that each part of the process can be handled separately and efficiently. The client layer is responsible for the user interface, where a user

can register, request access, and initiate communication. The application server layer manages session handling, user requests, and token generation. The blockchain layer stores and verifies authentication-related information through smart contracts, while the communication layer handles the secure transfer of voice data between users.

A one-time token is used as the main identity verification mechanism. When a user requests access, the server generates a token and the blockchain verifies whether that token is valid and unused. This prevents repeated use of the same access credentials and reduces the risk of replay attacks. Because the token is validated through a decentralized ledger, the system does not depend entirely on a single central authority for trust.

After successful verification, the system establishes a secure peer-to-peer voice connection using encrypted communication methods. This helps ensure that the voice data remains confidential during transmission and cannot be easily intercepted or modified. The peer-to-peer approach also reduces unnecessary traffic through intermediate servers, which improves communication efficiency and lowers the possibility of exposure.

The overall system design is intended to balance security, privacy, and usability. It protects user identity, supports trusted access control, and provides a practical framework for stealth voice communication. By separating authentication, blockchain validation, and voice transmission into distinct layers, the system becomes easier to manage, more reliable to test, and more adaptable for future improvements.

The system begins with user registration, where identity details are collected and prepared for verification. These details are then stored or linked in a blockchain-based environment so that they cannot be easily altered. Once the user is verified, the system allows access to the voice communication module. This ensures that only authenticated users can participate in the communication process.

After verification, the voice communication channel is established with security controls. The voice data is transmitted in a protected manner so that unauthorized users cannot intercept or misuse it. Stealth communication techniques are applied to reduce exposure of sensitive information, including user identity, call details, and communication patterns. This adds an extra layer of privacy beyond normal encryption.

The overall design is modular, which means each part of the system performs a specific task but works together as a complete framework. This makes the system easier to manage, more secure, and suitable for real-world use in applications where privacy and trust are essential.

3.2 User Registration

User registration is the first stage of the system, where a new user creates an account and submits the required identity information. In this project, registration is important because it establishes the initial trust relationship between the user and the communication platform. Only registered users should be allowed to proceed to the blockchain verification and voice communication stages

During registration, the system collects basic details such as username, contact information, and other identity-related data needed for authentication. This information is then linked to the blockchain-based verification process so that the user identity can be checked in a secure and tamper-resistant way. The registration step also helps prevent fake accounts and unauthorized access by ensuring that every user is uniquely identified.

A well-designed registration module should be simple, fast, and secure. It should guide the user through the required steps without exposing sensitive information. Once registration is completed, the user becomes eligible for verification and secure access to the stealth voice communication system.

Table 3.2

S. No.	Field	Description	Purpose
1	Username	Unique name chosen by the user.	To identify the user in the system.
2	Contact Details	Basic communication information.	To support account verification.
3	Identity Data	Required personal or system-linked details.	To confirm user authenticity.

S. No.	Field	Description	Purpose
4	Registration Status	Indicates whether the user is registered.	To control access to the next step.
5	Verification Link	Connects the user to blockchain validation.	To ensure secure authentication.

3.2 User Registration and Verification Fields

3.3 Blockchain Verification

Blockchain verification is the step where the system confirms a user's identity through a decentralized and tamper-resistant process. Instead of depending on a single central server, the identity information is stored or linked through blockchain records, which makes it much harder for attackers to alter, fake, or duplicate user credentials. This improves trust because the system can verify that the user is genuine before allowing access to voice communication.

Blockchain verification is the process of confirming the authenticity of a user or transaction through digital signatures and network consensus. The submitted request is first checked for validity, then broadcast to the network where multiple nodes verify it according to predefined rules. If the request is found to be genuine, it is approved and stored in the blockchain as a tamper-resistant record. This process improves trust, security, and resistance to unauthorized modification.

After this, the nodes perform consensus, which means they agree on whether the request should be accepted or rejected. If the request is confirmed as valid, it is added to the blockchain as a permanent and tamper-resistant record. Because the record is stored in linked blocks, it becomes very difficult to alter later without detection. This is one of the main reasons blockchain is considered secure and trustworthy.

In the context of your project, blockchain verification helps ensure that only authorized users can access the secure communication system. It protects against fake identities, unauthorized entry, and manipulation of stored records. This makes the system more trustworthy and suitable for secure voice communication applications where confidentiality is important.

In this project, blockchain verification can be understood as the bridge between registration and secure communication. After a user registers, the system checks the identity details against the blockchain-based record, often using decentralized identifiers or verifiable credentials. If the credentials are valid, the user is approved for communication; if not, access is denied. This process helps prevent impersonation, unauthorized access, and identity fraud while keeping the verification flow secure and privacy-preserving

Blockchain verification adds a secure trust layer to the system by checking whether a user's identity record is genuine before communication is allowed. Instead of depending on a central server, the verification process uses decentralized records, cryptographic keys, and tamper-resistant identity data, which makes it much harder for attackers to fake or alter credentials.

In a typical flow, the user first registers and submits identity information. The system then compares the stored blockchain hash or credential with the user's current identity proof. If the values match and the credential is valid, the user is approved; if not, access is denied. This process helps ensure that only verified users can join the voice communication channel, while also reducing the risk of impersonation and unauthorized entry.

3.4 Secure Voice Setup

Secure voice setup is the stage where the system creates a protected communication channel after the user has been verified. Its main purpose is to make sure that voice data travels safely between authorized users without being intercepted, altered, or overheard by unauthorized parties. In a secure communication system, this step is important because even if identity verification is successful, the voice channel itself still needs strong protection.

This setup usually includes encryption, secure signal and controlled access to the voice stream. Encryption protects the voice data during transmission, while secure signal helps establish the call in a trusted way. Access control ensures that only verified users can enter the voice session. In addition, the system may apply privacy controls so that the communication remains difficult to trace from outside.

For this project, secure voice setup acts as the bridge between blockchain verification and stealth communication. Once the user is authenticated through the blockchain-based identity process, the system creates a private voice session for communication. This keeps the conversation confidential and reduces the chances of attack, spoofing, or monitoring. The result is a communication environment that is both trusted and privacy-oriented.

Secure voice setup is the stage where the system prepares a protected communication channel after the user has been successfully verified. Its main purpose is to ensure that voice data can be exchanged safely without being intercepted, modified, or accessed by unauthorized users. This step is essential because even if identity verification is strong, the communication channel itself must still be protected from attack.

In a secure voice system, the voice session is usually established using encryption and secure signaling methods. Encryption protects the voice content during transmission, while secure signal helps create the connection in a trusted manner. Access control is also applied so that only verified users can join the session. These measures work together to make the voice communication reliable and confidential.

For this project, secure voice setup acts as the bridge between blockchain verification and stealth communication. Once the user is authenticated, the system creates a private voice channel for communication. This reduces the risk of eavesdropping, spoofing, and unauthorized monitoring. The result is a communication environment that is both secure and private, which is especially useful in sensitive applications such as defense, healthcare, corporate communication, and confidential messaging.

3.5 Stealth Communication Process

The stealth communication process is the stage where the system transmits voice data in a way that is difficult for outsiders to detect, track, or analyze. Its main purpose is not only to protect the voice content, but also to hide the communication pattern itself. This is important in secure applications because even if the voice is encrypted, attackers may still learn useful information from call timing, traffic flow, or user .

In this project, the stealth process adds privacy on top of blockchain-based identity verification. After a user is verified, the system sends the voice data through a protected path using

techniques such as encryption, packet masking, and tunneling. These methods help conceal the actual message and reduce the chances of interception or observation. The process also limits the exposure of metadata such as user identity, call duration, and communication route

The stealth communication process is especially useful in environments where confidentiality is critical. It helps ensure that only authorized users can communicate while keeping the transmission itself private. This makes the overall system stronger because it protects both access control and communication secrecy in one framework.

The stealth communication process is the part of the system that sends voice data in a way that is difficult for outsiders to notice, trace, or analyze. Its main purpose is not only to protect the message itself, but also to hide the communication pattern so that unauthorized users cannot easily detect that secure communication is taking place.

In this project, the process works after identity verification is completed. Once the user is authenticated, the system transmits voice through a protected channel using privacy-focused methods such as encryption, traffic masking, and hidden routing patterns. These methods reduce the chance of interception, observation, or traffic analysis.

Stealth communication is especially useful in sensitive environments where privacy is critical. It helps protect both the speaker identity and the communication content, while also limiting exposure of call details such as timing, duration, and route. This makes the system more resistant to eavesdropping and tracking.

At a broader level, the stealth communication process strengthens the whole project by adding privacy on top of blockchain-based authentication. Blockchain ensures that only genuine users are allowed to communicate, while stealth transmission ensures that the actual communication remains private and discreet. Together, they create a secure and trustworthy voice communication framework.

3.6 Summary

The stealth communication process sends voice data in a way that is private, protected, and difficult for outsiders to detect or analyze. In this project, it works after identity verification and helps make sure that the communication itself remains confidential, while also hiding details such as traffic patterns and session metadata.

Overall, it strengthens the system by adding privacy on top of blockchain-based authentication. Blockchain verifies who can communicate, and stealth transmission protects how the communication happens. Together, they create a secure and trustworthy voice communication framework.

The stealth communication process is the part of the system that keeps voice exchange private after the user has been verified. It does more than protect the audio itself, because it also tries to hide communication patterns, session details, and other information that could be useful to an attacker.

In this project, that means the voice data is sent through a secure and discreet channel so that unauthorized users cannot easily intercept, trace, or analyze it. This adds an extra layer of protection beyond blockchain-based identity verification, making the overall system stronger and more suitable for sensitive communication.

The proposed system integrates user authentication, verification, and secure communication into a single workflow. By using blockchain for validation, the system helps prevent unauthorized access and improves the integrity of the communication process. The design also supports modular implementation, making it easier to test, deploy, and extend in future .

CHAPTER 4

EXPERIMENTAL ANALYSIS AND DISCUSSION

This section presents the results of the proposed system after implementation and explains how effectively it performs in secure voice communication. It evaluates the system in terms of identity verification, privacy protection, communication reliability, and overall performance. The discussion helps show whether the proposed approach meets the intended objectives and how it improves over traditional methods.

The experimental analysis also examines how blockchain-based identity verification and stealth communication work together in the system. It highlights the strengths of the proposed model, identifies any limitations observed during testing, and explains the practical usefulness of the system in real-world scenarios.

The experimental analysis and discussion section presents the outcomes obtained after implementing the proposed system and explains how effectively it performs in practical use. This part evaluates the system based on key factors such as security, privacy, accuracy, response time, and reliability. It helps demonstrate whether the proposed model satisfies the main objectives of secure communication.

This section also compares the observed behavior of the system with the expected results. The discussion focuses on the effectiveness of blockchain-based verification and stealth communication in improving confidentiality and preventing unauthorized access. In addition, it highlights the strengths of the system, identifies limitations noticed during testing, and explains the relevance of the findings in real-world applications.

The experimental analysis and discussion section presents the performance of the proposed system after implementation and evaluates its effectiveness in a practical environment. It provides a detailed examination of the system's behavior under different conditions and shows how well it achieves the expected goals. This section is an important part of the report because it helps validate the proposed approach through observed results rather than only theoretical explanation.

The main purpose of this section is to assess the system in terms of security, reliability, efficiency, and user privacy. It discusses how blockchain-based identity verification strengthens access control and how stealth communication improves the confidentiality of voice transmission. The results are analyzed to understand the strengths of the system, the limitations encountered during testing, and the overall feasibility of the proposed model for real-world use.

In addition, this section compares the implemented system with the expected outcomes to determine whether the design is suitable for secure communication applications. It also highlights the significance of the experimental findings and explains how the combination of blockchain and stealth techniques contributes to a more trustworthy and privacy-preserving communication framework.

The experimental analysis and discussion section explains the performance of the proposed system after implementation and testing. It evaluates how effectively the system functions in a real or simulated environment and whether it meets the intended design goals. This section is

essential because it provides evidence of the system's practicality, efficiency, and security through observed outcomes.

The discussion focuses on important aspects such as authentication accuracy, communication reliability, privacy protection, and system responsiveness. It examines how the use of blockchain improves identity verification and how stealth communication enhances the confidentiality of transmitted voice data. The results obtained during testing are analyzed to understand the advantages of the proposed approach and to identify any challenges or limitations that may affect performance.

This section also helps establish the credibility of the proposed model by comparing expected behavior with actual performance. It shows whether the system is suitable for secure communication applications and explains how it performs under different conditions. Overall, the experimental analysis and discussion provide a clear understanding of the effectiveness and real-world value of the proposed system.

4.1 Experimental Setup

Experimental Setup refers to the arrangement of the system, conditions, and procedures used to test the proposed model. It describes how the experiment is carried out, what components are included, and what variables are observed during testing.

In a report, this section usually explains the environment in which the system was implemented, the hardware or software used, the test cases applied, and the steps followed to evaluate performance. Its purpose is to make the experiment clear and repeatable while ensuring that the results are measured under controlled conditions.

The **experimental setup** describes the environment, components, and conditions used to test the proposed system. It explains how the model was implemented and what arrangements were made to evaluate its performance in a controlled manner. This section is important because it gives a clear picture of the testing process and helps the reader understand how the results were obtained.

In this project, the experimental setup includes the software environment, the system modules, the input and output flow, and the communication process used for evaluation. The setup is designed to test the main functions of the system, such as user authentication, secure data handling, and privacy-preserving voice communication. Each component is configured to work together so that the overall system can be observed under realistic operating conditions.

Star



Initialize System



User Login/Register



Blockchain Verification



Authorized?

└─ Yes → Secure Voice Communication → Result Analysis → End

└─ No → Access Denied → Re-enter Details

The setup also ensures that the testing is consistent and reproducible. By maintaining controlled conditions, it becomes easier to analyze the performance of the system and identify any strengths or weaknesses. This section forms the foundation for the results and discussion that follow, since it explains the exact conditions under which the experiment was conducted.

The experimental setup describes the environment, resources, and procedures used to test the proposed system. It provides a structured view of how the implementation was carried out and how the performance of the system was measured. This section is important because it helps the reader understand the conditions under which the experiment was conducted and ensures that the results can be interpreted correctly.

In this project, the setup includes the software platform, system modules, test inputs, and communication flow used during evaluation. The proposed model is tested under controlled conditions so that its security, reliability, and efficiency can be observed clearly. Special attention is given to user authentication, secure communication, and privacy protection, since these are the main objectives of the system.

The setup also supports consistent testing by keeping the environment stable across all experiments. This makes it easier to compare results and identify the effectiveness of each module. Overall, the experimental setup forms the foundation for the analysis and discussion that follow in the report.

Table 4.1

Component	Description
System Environment	The platform used to run and test the proposed model.
User Interface	The interface used for registration, login, and communication.
Authentication Module	Verifies user identity before allowing access to the system.
SecureCommunication Module	Handles private and protected voice communication.
Test Cases	Different input scenarios used to evaluate performance.
Evaluation Criteria	Measures such as security, reliability, response time, and privacy.

4.1 System Components and Evaluation Criteria

4.2 Performance Evaluation

Performance evaluation explains how well the proposed system works after implementation. It measures whether the system achieves its goals in terms of security, privacy, efficiency, and

reliability. This part is important because it shows the actual behavior of the system rather than only describing its design.

In this project, performance evaluation can focus on several factors such as authentication accuracy, response time, communication stability, and privacy protection. For example, the system can be tested to see how quickly a user is verified, how smoothly voice communication happens, and how effectively unauthorized access is prevented. These measures help determine whether the system is practical for real use and whether it performs better than a traditional communication method.

A good performance evaluation section also explains the test conditions used during analysis. This may include the number of users, sample messages, network conditions, and repeated trials. By observing the system under controlled conditions, it becomes easier to identify strengths, limitations, and possible improvements.

The performance evaluation of the proposed system is carried out to assess its efficiency and effectiveness under different test conditions. It examines how well the system performs in terms of identity verification, secure communication, and privacy preservation. The evaluation also measures response time and reliability to ensure that the system functions smoothly during operation.

The results obtained from performance testing help verify whether the proposed approach satisfies the security requirements of the application. They also provide useful information about possible improvements that can be made in future versions. Overall, the performance evaluation confirms the practical usefulness of the system and supports the effectiveness of the proposed design.

Table 4.2

Metric	What It Measures	Importance
Authentication Accuracy	Whether only valid users are allowed access	Ensures security and trust

Metric	What It Measures	Importance
Response Time	Time taken for login or verification	Shows system efficiency
Communication Reliability	Stability of voice transmission	Confirms smooth operation
Privacy Protection	Ability to prevent data leakage	Protects confidential communication
Unauthorized Access Prevention	Blocks fake or unknown users	Strengthens system security

4.2 Security and Performance Evaluation Metrics

The performance evaluation of the proposed system is carried out to assess its efficiency and effectiveness under different test conditions. It examines how well the system performs in terms of identity verification, secure communication, and privacy preservation. The evaluation also measures response time and reliability to ensure that the system functions smoothly during operation.

The results obtained from performance testing help verify whether the proposed approach satisfies the security requirements of the application. They also provide useful information about possible improvements that can be made in future versions. Overall, the performance evaluation confirms the practical usefulness of the system and supports the effectiveness of the proposed design.

4.3 Result Discussion

The result discussion explains the meaning of the experimental outcomes obtained after testing the proposed system. It interprets whether the system performed as expected and how effectively it achieved secure and private communication. This section connects the raw results with the objectives of the project and gives a clear understanding of the system's practical value.

In this project, the results may show that the blockchain-based authentication process successfully verified legitimate users and prevented unauthorized access. This indicates that the security mechanism works effectively and improves trust in the system. The secure communication process may also demonstrate that voice data is transmitted with better privacy and reduced risk of interception.

The discussion should also mention any limitations observed during testing. For example, slight delay in verification, dependence on network quality, or performance variation under heavier load can be noted as practical issues. Including these points makes the evaluation more realistic and balanced.

Overall, the result discussion should conclude that the proposed system performs well in maintaining confidentiality, reliability, and secure access. It shows that the combination of blockchain verification and stealth communication provides a strong approach for privacy-preserving voice communication.

The result discussion explains what the experimental outcomes mean and how they reflect the performance of the proposed system. It goes beyond simply stating that the system worked and instead interprets whether the design successfully achieved secure, private, and reliable communication. This part is important because it connects the testing results with the main objectives of the project.

In this system, the results are generally expected to show that authentication is carried out properly, only valid users are allowed to access the platform, and communication remains protected from unauthorized interception. If the blockchain-based identity verification works correctly, it proves that the system has strong access control. If the voice communication remains confidential during transmission, it shows that the stealth communication method is effective in preserving privacy.

The result discussion should also highlight how the system behaves under different test conditions. For example, when the number of users increases or when network quality changes, the system may show slight variations in response time or stability. These observations are useful because they help identify both the strengths of the system and the areas that may need further improvement. A good result discussion does not only mention positive outcomes; it also presents practical limitations in a balanced way.

Another important point is consistency. If the system produces the same secure results across multiple tests, it means the model is dependable and suitable for real-world use. If any delay or minor disruption is observed, it should be explained as a performance factor rather than a failure. This makes the evaluation more realistic and academically strong.

Overall, the result discussion should conclude that the proposed system performs effectively in maintaining secure access, privacy, and reliable communication. The combination of blockchain verification and stealth communication improves trust in the system and makes it suitable for privacy-sensitive applications.

The results indicate that the proposed approach is effective in solving the main problems of secure communication, especially identity fraud and privacy leakage. By using blockchain, the system ensures that only trusted users can participate, which improves reliability. By using stealth communication, it reduces the chances of data exposure, which is important for confidential voice exchange.

Table 4.3

Aspect	What Was Observed	Meaning of the Result
User Authentication	Valid users were successfully verified.	Access control is working properly.
Unauthorized Access	Invalid users were blocked from entering.	Security is strengthened.
Voice Privacy	Communication remained confidential during transmission.	Privacy protection is effective.
Response Time	Slight delay may appear during verification.	Performance is acceptable, but optimization may help.

Aspect	What Was Observed	Meaning of the Result
System Stability	The system worked consistently in repeated tests.	The model is reliable.
Overall Output	Results matched the goals of the proposed design.	The system is practically useful.

4.3 System Results and Observation Analysis

The proposed system. It analyzes whether the The result discussion explains the practical meaning of the experimental outcomes obtained after testing system performed according to the expected objectives and how effectively it supported secure and private communication. This section is important because it does not just present the results; it interprets them and shows what they mean in the context of the project.

The experimental results indicate that the proposed system performs well in controlling access, protecting user identity, and maintaining privacy during communication. The authentication process successfully distinguishes valid users from unauthorized users, which improves trust in the system. At the same time, the secure voice communication mechanism helps ensure that the transmitted data remains confidential and less exposed to external threats.

The discussion of results also shows that the system maintains a good level of stability during repeated testing. This means the proposed model can produce consistent outputs under similar conditions, which is an important requirement for practical deployment. If minor delay or variation is observed during authentication or communication, it can be considered a normal performance factor that may be improved in future versions.

Another important observation is that the integration of blockchain verification and stealth communication provides stronger protection than a traditional voice communication setup. Blockchain enhances identity security by making unauthorized access more difficult, while stealth communication adds an additional privacy layer to the communication process. Together, these features improve both safety and reliability.

Overall, the result discussion confirms that the proposed system is effective for secure communication applications. The findings show that it supports confidentiality, prevents

unauthorized access, and performs consistently under the tested conditions. This makes the system suitable for environments where privacy and trust are essential.

Table 4.3

Aspect	Observation	Discussion
Authentication	Valid users were successfully identified.	The access control mechanism works correctly.
Unauthorized Access	Invalid users were blocked.	Security is improved through strict verification.
Privacy Protection	Voice data remained confidential.	The stealth communication method is effective.
Consistency	Similar results were obtained in repeated tests.	The system is stable and reliable.
Performance	Minor delay may occur during verification.	The system is efficient, with room for optimization.
Overall Effectiveness	Results matched the project goals.	The proposed model is practical and useful.

4.3 Discussion of Test Results and System Effectiveness

The result discussion of the proposed system shows that the model performs effectively in achieving secure and private communication. The authentication module successfully verifies legitimate users and prevents unauthorized access, while the stealth communication process helps maintain confidentiality during data transmission. The results also indicate that the system is stable and reliable across repeated tests. Although minor delays may be observed in some cases, the overall performance remains satisfactory. Hence, the experimental results confirm that the proposed system is suitable for secure communication applications.

4.4 Analysis of Findings

The analysis of findings explains what the experimental results reveal about the proposed system and whether it meets the expected objectives. It interprets the test outcomes in a meaningful way, showing how the system behaves in terms of security, privacy, reliability, and efficiency. This section is important because it connects the observed results with the overall purpose of the project.

The findings suggest that the proposed system is effective in providing secure access through blockchain-based authentication. Only authorized users are allowed to enter the system, which reduces the risk of identity misuse and unauthorized entry. This shows that the verification mechanism is strong and suitable for applications that require trusted access control.

The results also indicate that the stealth communication approach helps protect voice data during transmission. By reducing the chances of interception or exposure, the system improves privacy and confidentiality. This is especially useful in situations where sensitive communication needs to be protected from external threats.

Another important finding is that the system performs consistently under the tested conditions. Repeated trials show similar behavior, which means the model is stable and dependable. Even if small delays are observed during verification or communication, the overall performance remains acceptable for practical use.

From the findings, it can be concluded that the combination of blockchain and stealth communication offers a stronger solution than traditional methods. The blockchain layer improves trust and security, while the stealth layer enhances privacy and confidentiality. Together, they create a well-balanced system that is effective for secure voice communication.

Table 4.4

Finding	Observation	Interpretation
User Authentication	Only valid users were granted access.	The security mechanism is effective.

Finding	Observation	Interpretation
Unauthorized Access Prevention	Invalid users were blocked.	The system protects against misuse.
Voice Privacy	Communication remained confidential.	The stealth method works well.
System Stability	Similar results appeared in repeated tests.	The system is reliable.
Performance	Minor delay may occur in some steps.	Efficiency is good, though optimization may help.
Overall Outcome	Results supported the project goals.	The proposed model is practical and effective.

4.4 Findings and Interpretation of System Evaluation

The analysis of findings presents the meaning of the experimental results and explains what they reveal about the performance of the proposed system. It helps determine whether the system has successfully achieved its main goals, such as secure access, privacy protection, and reliable communication. This section is important because it gives a deeper understanding of the results instead of simply listing them.

From the findings, it can be observed that the proposed system performs effectively in verifying users and preventing unauthorized access. The blockchain-based authentication mechanism ensures that only legitimate users can participate in the communication process. This strengthens the overall security of the system and reduces the chances of identity fraud or misuse.

The findings also show that the stealth communication method contributes significantly to privacy preservation. Since the voice data is transmitted in a more secure and less exposed manner, the risk of interception is reduced. This makes the system suitable for situations where confidential communication is required.

Another important observation is that the system remains stable during repeated testing. Consistent results indicate that the model is dependable and can function properly under similar conditions. Even if slight delays are present in verification or communication, the system still maintains acceptable performance, which suggests that it is practical for use.

Overall, the analysis of findings confirms that the proposed system is effective in combining security and privacy features. The integration of blockchain and stealth communication provides a stronger solution than conventional voice communication methods. The findings support the conclusion that the system is both useful and reliable for secure communication applications.

The analysis of findings indicates that the proposed system performs well in terms of security, privacy, and reliability. The blockchain-based authentication successfully verifies users, while the stealth communication mechanism helps maintain confidentiality during voice transmission. The experimental results also show that the system is stable and produces consistent outputs under repeated tests. Therefore, the findings confirm that the proposed model is effective for secure communication applications.

4.5 Advantages of the Proposed System

The proposed system offers strong security by combining blockchain-based authentication with stealth communication. This makes it more effective than a traditional voice communication system, especially when privacy and trust are important.

One major advantage is that only verified users can access the system. The blockchain layer helps prevent unauthorized entry, identity misuse, and tampering with user records. This improves the reliability of the authentication process and increases user confidence.

Another advantage is privacy protection during communication. The stealth communication mechanism helps reduce the risk of interception and exposure of sensitive voice data. This makes the system suitable for confidential conversations in secure environments.

The system is also more transparent and dependable because blockchain creates a secure and traceable verification process. In addition, the modular design makes the system easier to manage, test, and extend in future updates. Overall, the proposed system provides a balanced combination of security, privacy, and usability.

The proposed system offers several important advantages that make it more effective than conventional communication approaches. Its main strength lies in the combination of blockchain-based authentication and stealth communication, which together improve both security and privacy. This makes the system suitable for applications where confidential communication is necessary.

One major advantage is that the system allows only authorized users to access the platform. Since identity verification is handled through blockchain, the records are more secure, difficult to alter, and less vulnerable to unauthorized access. This reduces the risk of identity theft, fake user registration, and tampering with authentication data

Another advantage is the protection of voice communication from external threats. The stealth communication mechanism helps keep transmitted data private and less exposed to interception. This is especially useful in sensitive environments where users need to exchange information securely without revealing their communication details to outsiders.

The system also provides better trust and transparency. Because blockchain stores verification-related information in a secure and traceable manner, it becomes easier to trust the identity validation process. This improves the overall credibility of the system and makes it more reliable for practical use.

In addition, the modular structure of the proposed system makes it easier to maintain and improve. Each component can be tested and updated separately, which supports future development and scalability. Overall, the system is efficient, secure, privacy-focused, and well-suited for real-world secure communication scenarios.

Table 4.5

Advantage	Description
Strong User Authentication	Only verified users can access the system.
High Security	Blockchain reduces tampering and unauthorized access.
Privacy Protection	Stealth communication keeps voice data confidential.
Better Trust	Verification records are secure and traceable.
Reliable Operation	The system performs consistently under test conditions.
Easy Maintenance	Modular design supports future updates and improvements.
Scalability	The system can be extended for larger applications.

4.5 Advantages of the Proposed System

The proposed system provides a strong and effective approach for secure communication by combining blockchain technology with stealth communication. One of its biggest advantages is improved security, since only authenticated users are allowed to access the system. This reduces the chances of unauthorized entry, fake identity usage, and tampering with user information.

Another important advantage is privacy protection. The stealth communication method helps keep voice data hidden from unwanted access, making the system suitable for confidential conversations. This is especially useful in situations where sensitive information must be shared without exposing the communication to third parties.

The system also improves trust and reliability. Blockchain maintains a secure and traceable verification process, which makes the authentication stage more dependable. Because the records are difficult to alter, the system becomes more transparent and resistant to manipulation.

In addition, the proposed system is flexible and easy to manage because of its modular structure. Each part of the system can be tested, updated, or improved separately without affecting the entire application. This makes the design easier to maintain and more suitable for future enhancements

The system is also useful in practical scenarios where both security and confidentiality are required. It can support environments such as personal secure communication, organizational messaging, and privacy-sensitive exchanges. Overall, the proposed system offers a balanced combination of authentication, privacy, trust, and usability.

Table 4.5

Advantage	Description
Strong Authentication	Ensures that only verified users can access the system.
Better Security	Blockchain helps prevent tampering and unauthorized access.
Privacy Protection	Stealth communication keeps voice data confidential.
Increased Trust	Secure and traceable records improve reliability.
Easy Maintenance	Modular design supports updates and modifications.
Practical Use	Suitable for secure and privacy-sensitive communication.
Future Expansion	The system can be extended for larger applications.

4.5 Advantages and Practical Benefits of the Proposed System

4.6 Limitations Observed

The proposed system has some limitations that were noticed during testing. These limitations do not reduce the usefulness of the system, but they show areas where improvement is still possible. Mentioning them in the report makes the analysis more realistic and balanced.

One limitation is that the system may depend heavily on network stability. Since secure communication and verification processes are performed through connected modules, poor

network conditions can cause delay or interruption. This may affect the smoothness of real-time voice communication.

Another limitation is that blockchain-based verification can introduce some processing delay. Although it improves security, it may take slightly longer than a simple login method. This can be noticeable when many users try to access the system at the same time.

The system may also require more resources compared to a conventional communication setup. Because it combines authentication, secure storage, and communication protection, the implementation can be more complex. This may make deployment and maintenance a little harder in low-resource environments.

In addition, the stealth communication feature may need careful tuning to perform efficiently in different scenarios. If the configuration is not optimized, the system may experience reduced speed or variation in performance. Therefore, further refinement may be needed before large-scale use.

The proposed system, while effective, has a few limitations that were noticed during the testing phase. These limitations are mainly related to performance, network dependence, and implementation complexity. Including them in the report is important because it provides a fair and realistic view of the system.

One major limitation is that the system depends on a stable network connection for smooth operation. Since the communication process involves secure verification and protected voice exchange, any interruption in the network can affect responsiveness. In a weak network environment, the system may experience delay or instability during authentication or communication.

Another limitation is the extra time required for blockchain-based verification. Although this method improves security and trust, it may take longer than a simple centralized login process. This can slightly affect the overall speed of access, especially when multiple users attempt to connect at the same time.

The system may also consume more computational resources because it combines multiple security features in one platform. The use of secure authentication, privacy protection, and communication handling makes the system more complex than a standard application. As a

result, deployment and maintenance may require more careful configuration and higher system support.

In addition, the stealth communication component may need further optimization for large-scale use. While it works effectively in controlled conditions, performance can vary depending on the environment and usage load. This means that future improvements may be needed to make the system more efficient and scalable.

Overall, the limitations observed are not major failures but practical constraints that can be improved in future work. They mainly indicate that the system is strong in security and privacy, but further optimization is needed for better speed, scalability, and resource efficiency.

Table 4.6

Limitation	Explanation
Network Dependence	The system may slow down if the internet connection is unstable.
Verification Delay	Blockchain authentication can take more time than traditional login methods.
Higher Resource Use	The system may need more processing power and memory.
Complexity	Multiple modules make the system harder to manage and maintain.
Scalability	Performance may reduce when the number of users increases.
Optimization Requirement	The stealth communication process may need tuning for better efficiency.

4.6 Limitations of the Proposed System

The proposed system is effective in improving secure communication, but it still has certain limitations that should be acknowledged. These limitations mainly relate to network dependence, processing delay, system complexity, and scalability. Including these points makes the report more complete and balanced.

One limitation is that the system requires a stable and reliable network connection to function smoothly. Since the communication process involves secure verification and protected voice transmission, poor connectivity can affect performance. If the network is weak or unstable, the system may respond slowly or experience interruptions during operation.

Another limitation is the additional time required for blockchain-based authentication. Although this method improves security and reduces unauthorized access, it may take longer than a basic login system. This can slightly affect the speed of the overall process, especially when many users are accessing the system at the same time.

The system also has a higher level of complexity because it combines multiple security functions in one platform. Authentication, privacy protection, and secure communication all need to work together properly. This increases the effort needed for implementation, testing, and maintenance compared to simpler communication systems.

In addition, the system may require more resources such as memory, processing power, and configuration support. This can make deployment more difficult in low-resource environments. The stealth communication component may also need further tuning to perform efficiently in different operating conditions.

Overall, the limitations observed are practical concerns rather than major failures. They show that the system is strong in security and privacy, but still needs optimization for faster performance, better scalability, and easier deployment in real-world environments.

Table 4.6

Limitation	Explanation
Network Dependence	Performance may decrease when the connection is unstable.
Verification Delay	Blockchain authentication can take extra time.
System Complexity	Multiple modules make implementation and maintenance harder.

Limitation	Explanation
Higher Resource Requirement	The system may need more processing power and memory.
Scalability Issue	Performance may vary as the number of users increases.
Tuning Requirement	Stealth communication may need optimization for better efficiency.

4.6 Limitations and Challenges of the Proposed System

The proposed system has some limitations observed during testing. It depends on stable network connectivity, and blockchain-based verification may introduce slight delays. The system is also more complex and may require additional resources compared to traditional communication methods. These limitations can be improved in future work through optimization and better system design.

4.7 Summary

The summary section briefly brings together the main points discussed in the experimental analysis. It highlights that the proposed system performs effectively in secure communication by combining blockchain-based authentication with stealth communication. This combination improves security, protects privacy, and helps prevent unauthorized access.

The experimental results also show that the system is reliable and consistent under the tested conditions. Although some limitations such as delay, network dependence, and higher resource usage were observed, the overall performance remains satisfactory. These findings confirm that the proposed system is suitable for privacy-sensitive communication applications and has good potential for future improvement.

The proposed system demonstrates that secure communication can be improved by combining blockchain-based authentication with stealth communication techniques. This combination helps ensure that only authorized users can access the system while keeping voice data private during transmission. As a result, the system addresses two major concerns in modern communication: security and confidentiality.

The experimental analysis shows that the system performs well under controlled test conditions. It provides consistent authentication, maintains communication privacy, and works reliably across repeated tests. Although some limitations were observed, such as slight delay, network dependence, and higher resource requirements, these do not outweigh the overall effectiveness of the model.

The proposed system effectively combines blockchain-based authentication and stealth communication to provide secure and private voice communication. The experimental results show that the system is reliable and consistent, although some limitations such as delay and network dependence were observed. Overall, the system is suitable for secure communication applications and has strong potential for future improvement.

CHAPTER 5

CONCLUSION AND FUTURE WORK

The introduction presents the main idea of the project and explains the purpose of the proposed system. It gives an overview of how blockchain-based authentication and stealth communication are combined to provide secure and private voice communication. This section sets the background for the report and explains why the topic is important in today's communication systems.

The proposed system successfully demonstrates a secure approach to voice communication by combining blockchain-based authentication with stealth communication. It improves access control, protects privacy, and reduces the risk of unauthorized use. The experimental results indicate that the system is effective, reliable, and suitable for applications where confidential communication is important.

The study also shows that the system has some practical limitations, such as slight delay, network dependence, and higher resource requirements. Even so, the overall performance remains satisfactory and supports the feasibility of the proposed design. Therefore, the system can be considered a strong solution for secure and privacy-preserving communication.

The proposed system is designed to improve security, privacy, and reliability in voice communication. By using blockchain, the system ensures that only authorized users can access the platform, while stealth communication helps protect the transmitted voice data from unauthorized interception. Together, these features create a stronger and more trustworthy communication model.

In addition, the introduction highlights the need for secure communication in environments where confidentiality is essential. Traditional communication systems may be vulnerable to identity misuse, data leakage, and unauthorized access. Therefore, the proposed approach offers a practical solution that combines modern security techniques to address these challenges effectively.

This project is important because conventional communication systems may face problems such as unauthorized access, identity misuse, and privacy leakage. In many practical situations, users need a communication platform that not only works efficiently but also protects their data from external threats. The proposed model addresses these concerns by creating a safer and more reliable communication environment.

In addition, the introduction provides the foundation for the rest of the report by explaining why the system was developed and what it is expected to achieve. It prepares the reader for the experimental analysis, performance evaluation, and discussion that follow in later sections. Overall, the project aims to deliver a secure, privacy-preserving, and practical communication solution.

5.1 Conclusion

The proposed system effectively combines blockchain-based authentication with stealth communication to provide secure and private voice communication. It improves user verification, reduces the risk of unauthorized access, and protects sensitive data during transmission. The overall design demonstrates that the system can meet the requirements of secure communication in a practical way.

The experimental analysis shows that the system performs reliably under the tested conditions, although minor limitations such as delay and network dependence were observed. Even with these constraints, the system remains useful and efficient for privacy-sensitive applications. Therefore, the proposed model can be considered a strong and effective solution for secure voice communication.

The proposed system successfully demonstrates a secure and practical method for voice communication by combining blockchain-based authentication with stealth communication. This approach improves the overall security of the system by ensuring that only authorized users can gain access. At the same time, it protects the confidentiality of voice data during transmission, which is essential for privacy-sensitive communication environments.

The experimental analysis and discussion show that the system performs effectively under the tested conditions. It maintains reliable authentication, supports secure communication, and helps prevent unauthorized access or data exposure. Although some limitations such as slight delay, network dependence, and higher resource usage were observed, these do not reduce the overall usefulness of the system. Instead, they highlight areas where future improvements can be made.

In conclusion, the proposed model provides a strong combination of security, privacy, and reliability. It is suitable for applications where confidential communication is required and shows good potential for real-world use. The results confirm that integrating blockchain with stealth communication is an effective approach for building a more trustworthy communication system.

The proposed system successfully achieves its main objective of providing secure and private voice communication through the integration of blockchain-based authentication and stealth

communication. By using blockchain, the system ensures that only authenticated users are allowed to access the platform, which significantly reduces the chances of unauthorized entry and identity misuse. At the same time, stealth communication helps protect the transmitted voice data from interception, thereby strengthening privacy and confidentiality.

The experimental results indicate that the system performs reliably and consistently under the tested conditions. It supports secure access, maintains communication privacy, and demonstrates practical usefulness in real-world scenarios where confidential communication is required. Although some limitations such as delay, network dependence, and resource overhead were observed, the system still shows strong potential as a secure communication solution.

Overall, the proposed model provides a balanced combination of security, trust, and privacy. It is an effective approach for applications that require protected voice communication and can be further improved in future work for better speed, scalability, and efficiency. The study confirms that integrating blockchain with stealth communication is a promising direction for developing advanced secure communication systems.

In conclusion, the proposed system offers a reliable and secure way to handle voice communication by combining blockchain authentication with stealth-based privacy protection. The design improves user verification, prevents unauthorized access, and protects sensitive information during transmission. The experimental analysis confirms that the system works effectively under controlled conditions and provides a strong foundation for secure communication applications. Therefore, the proposed approach can be considered practical, effective, and suitable for future enhancement.

5.2 Future Work

Future work can focus on improving the speed and efficiency of the proposed system. Since blockchain verification may introduce some delay, optimization techniques can be applied to reduce response time and make the communication process smoother.

Another important direction is scalability. The system can be extended to support a larger number of users and handle higher traffic without affecting performance. This would make it more practical for real-world deployment in organizations or secure communication platforms.

Security can also be strengthened further by integrating advanced encryption methods and adaptive authentication mechanisms. These enhancements would provide an additional layer of protection against unauthorized access and privacy threats.

Future development can also include stronger encryption methods and more advanced authentication techniques. These additions would improve protection against unauthorized access and make the system even more reliable in sensitive environments. In addition, better error handling and adaptive security controls could be introduced to improve robustness.

The user experience can also be improved in future versions. A more intuitive interface, mobile compatibility, and easier navigation would make the system more accessible to different types of users. These improvements would increase the practicality of the model and make it more suitable for real-world deployment.

Table 5.2

Area	Improvement
Speed	Reduce blockchain verification delay and improve response time.
Scalability	Support more users and simultaneous communication sessions.
Security	Add advanced encryption and stronger authentication methods.
Reliability	Improve error handling and system stability.
Usability	Enhance interface design and ease of use.
Deployment	Make the system suitable for broader real-world applications.

5.2 Future Enhancements and Improvements

Future work can focus on reducing delay, improving scalability, and strengthening security. The system can also be enhanced with advanced encryption, better authentication, and a more user-friendly interface. These improvements would make the proposed model more efficient, practical, and suitable for large-scale secure communication.

5.3 Summary

The proposed system presents a secure and privacy-focused approach to voice communication by combining blockchain-based authentication with stealth communication. It improves user verification, protects confidential voice data, and reduces the risk of unauthorized access.

The experimental analysis shows that the system performs reliably under the tested conditions, though minor limitations such as delay, network dependence, and resource usage were observed. Overall, the model is practical, effective, and suitable for secure communication applications.

The proposed system provides a secure and reliable method for voice communication by integrating blockchain-based authentication with stealth communication. This combination improves access control, ensures that only authorized users can enter the system, and helps protect sensitive voice data from unauthorized exposure. As a result, the system addresses two major concerns in communication platforms: security and privacy.

The experimental analysis shows that the system performs well under the tested conditions. It maintains stable authentication, supports confidential communication, and works consistently across repeated trials. Although some practical limitations such as delay, network dependence, and higher resource usage were observed, the overall performance remains satisfactory and useful for real-world applications.

The proposed system effectively combines blockchain-based authentication and stealth communication to provide secure and private voice communication.

REFERENCES

- [1] Hand gesture recognition communication system: For silent speakers - Gesture-to-speech for discreet talking, like hidden call triggers. <https://ieeexplore.ieee.org/document/6887815>
- [2] Hand Gesture Communication using Deep Learning - Gesture learning for interfaces, aligns with sensor triggers. <https://ieeexplore.ieee.org/document/9322784>
- [3] SOM-based hand gesture recognition for virtual interactions - ML for gesture detection, core to your algorithms. <https://ieeexplore.ieee.org/document/5759659>

- [4] WISE: Waveform Independent Signal Embedding for Covert Communication - Hidden signals for LPD, matches zero-trace VoIP. <https://ieeexplore.ieee.org/document/10360170>
- [5] Design And Implementation Of Gesture Based Human Computer Interaction - Gesture HCI for mobile/wearables. <https://ieeexplore.ieee.org/document/9404672>
- [6] The design and implementation of invisible eavesdropping - Hidden mobile audio access. <https://ieeexplore.ieee.org/document/7015423>
- [7] Gesture Recognition Framework for Teleoperation of Infrared Devices - Wearable gesture controls. IEEE Xplore
- [8] Invisible messenger: visually steerable sound beam forming - Hidden audio privacy tech. <https://ieeexplore.ieee.org/document/1389770>
- [9] Privacy-Preserving Covert Communication Using Encrypted Wearable Gesture Recognition - Encrypted gestures for covert channels. <https://arxiv.org/pdf/2602.07936.pdf>
- [10] Detecting Intrusions using System Calls: Alternative Data Models - Background service security. <https://www.computer.org/csdl/proceedings-article/sp/1999/01760133/12OmNwCaCz2>

APPENDIX A - SOURCE CODE

```
const express = require("express");

const http = require("http");

const { Server } = require("socket.io");

const crypto = require("crypto");

const cors = require("cors");
```

```
const app = express();

app.use(express.json());

app.use(cors());


app.use(express.static("public"));


const server = http.createServer(app);


const io = new Server(server, {

  cors: {

    origin: "*",

    methods: ["GET", "POST"]

  }

});


// Ephemeral storage

let rooms = {};

let tokens = {};
```

//  Generate Link

```
app.post("/generate-link", (req, res) => {

  const token = crypto.randomBytes(4).toString("hex");

  tokens[token] = {

    expiry: Date.now() + 15 * 60 * 1000 // 15 min

  };

  const baseUrl = process.env.BASE_URL || "https://stealth-voice-system.netlify.app/";

  res.json({

    token,

    link: `${baseUrl}/join/${token}`

  });

});

//  Verify Token

app.post("/verify-token", (req, res) => {

  const { token } = req.body;
```

```
if (!tokens[token]) return res.json({ success: false });

if (Date.now() > tokens[token].expiry) {

    delete tokens[token];

    return res.json({ success: false });

}

res.json({ success: true });

});

// 📡 WebRTC signaling

io.on("connection", (socket) => {

    socket.on("join", (token) => {

        socket.join(token);

        if (!rooms[token]) rooms[token] = [];

        rooms[token].push(socket.id);

        // When 2 users join → start
```

```
if (rooms[token].length === 2) {  
  
    io.to(rooms[token][0]).emit("ready", true);  
  
    io.to(rooms[token][1]).emit("ready", false);  
  
}  
  
// Auto cleanup  
  
setTimeout(() => {  
  
    delete rooms[token];  
  
    delete tokens[token];  
  
}, 15 * 60 * 1000);  
  
});  
  
socket.on("offer", ({ token, offer }) => {  
  
    socket.to(token).emit("offer", offer);  
  
});  
  
socket.on("answer", ({ token, answer }) => {  
  
    socket.to(token).emit("answer", answer);  
  
});
```

```
socket.on("ice", ({ token, candidate }) => {
```

```
    socket.to(token).emit("ice", candidate);
```

```
});
```

```
socket.on("disconnect", () => {
```

```
    for (let t in rooms) {
```

```
        rooms[t] = rooms[t].filter(id => id !== socket.id);
```

```
        if (rooms[t].length === 0) delete rooms[t];
```

```
    }
```

```
});
```

```
});
```

```
const PORT = process.env.PORT || 10000;
```

```
server.listen(PORT, () => {
```

```
    console.log("🚀 Server running on port", PORT);
```

```
});
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<title>Indie Secure Call</title>
```

</head>

<body style="background:#111;color:white;text-align:center;font-family:sans-serif">

<h2>🔒 Indie Call</h2>

<div id="home">

<button onclick="generateLink()">Generate Call Link</button>

<p id="link"></p>

<input id="tokenInput" placeholder="Enter Token">

<button onclick="verify()">Join Call</button>

</div>

<div id="call" style="display:none;">

<h3 id="status">Connecting...</h3>

<audio id="audio" autoplay></audio>

</div>

<div id="call" style="display:none;">

<h3 id="status">Connecting...</h3>

<audio id="audio" autoplay></audio>

</div>

<script src="https://cdn.socket.io/4.7.2/socket.io.min.js"></script>

<script>

const SERVER = "https://stealth-voice-system.onrender.com"; // 🔥 PUT YOUR REAL
BACKEND URL

const socket = io(SERVER);

let pc;

let stream;

let token;