International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Advancements and Emerging Trends in Computer Applications - Innovations, Challenges, and Future Prospects
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# VoIP without the Internet: Enhancing PBX Over Wi-Fi

**Mayur Indurkar**

PG Student, Department of Computer Application, G. H. Raisoni University, Amravati, Maharashtra, India

**ABSTRACT**

Voice over Internet Protocol (VoIP) is an innovative communication technology that allows for the transfer of voice and multimedia content via IP networks. However, traditional VoIP setups often rely on internet connectivity, raising concerns about security, reliability, and latency. This research presents a practical solution—integrating VoIP with an IP PBX system over a **secure Virtual Private Network (VPN) within a local Wi-Fi network**, eliminating the need for internet access. By ensuring secure internal communication, this approach is ideal for enterprises and institutions requiring a controlled communication environment. Through network simulations and performance analysis, we examine security measures, delay factors, and overall system efficiency. The results confirm that VoIP over a local Wi-Fi VPN enhances security while maintaining low latency, making it a robust alternative to internet-dependent VoIP solutions.

***KEYWORDS:*** *VoIP, IP PBX, Secure VPN, SIP, Network Security, Delay Analysis, Local Wi-Fi Network*

## I. INTRODUCTION

The internet has transformed communication through VoIP to facilitate global data and voice transfer. Conventional telecommunication infrastructure is plagued with issues of cost, security exposure, and inefficiency in networks. VoIP offers an economic alternative with advantages of voice call, video conference, and real-time communication. Security threats and Quality of Service (QoS) problems, however, make it imperative for strong solutions. This article discusses the integration of VoIP with an IP PBX system over a secure VPN for improving communication security and minimizing network delay. The most important aspect of this model is that it runs on a local area through Wi-Fi, without any internet connection requirement, but maintaining secure internal communication.

### VOIP:-

VOIP is a solid technology available since some years that allows people to communicate via voice using the IP protocol instead of telephone lines [7]. VOIP is a technology for communicating using "Internet protocol" instead of traditional analog systems. Some VOIP services need only a regular phone connection, while others allow you to make telephone calls using an Internet connection instead [4]. Some VOIP services may allow you only to call other people using the same service, but others may allow you to call any telephone number - including local, long distance, wireless, and international numbers.

Voice over IP – the transmission of voice over packet-switched IP networks – is one of the most important emerging trends in telecommunications. As with many new technologies, VOIP introduces new security.

### IP-PBX

Before VOIP, the PBX was the mainframe of corporate telephony. PBX stands for Private Branch Exchange or Premises Business Exchange. An IP PBX is a private branch exchange (telephone switching system within an enterprise) that switches calls between VOIP (voice over Internet Protocol or IP) users on local lines while allowing all users to share a certain number of external phone lines. The typical IP PBX can also switch calls between a VOIP user and a traditional telephone user, or between two traditional telephone users in the same way that a conventional PBX does. The abbreviation may appear in various texts as IP-PBX, IP/PBX, or IPPBX [4]. With a conventional PBX, separate networks are necessary for voice and data communications.

### Aim of Research

In recent years, there has been considerable debate within the sector regarding the merging of voice and data and the advantages and disadvantages of transmitting voice through a data network. This white paper aims to explore the concept of voice over IP telephony utilizing an IP/PBX framework. The goal of this investigation is to develop an optimal IP PBX solution that can incorporate internet telephony alongside other communication services, including email, file transfer protocol, and instant messaging, all functioning harmoniously within the same exchange platform or server. Moreover, this solution will facilitate communication via Wi-Fi without requiring an internet connection, allowing for local voice and data transmission in a specified setting. This system can be deployed in an environment such as our institution, with our department serving as a case in point.

## II. EXISTING RESEARCH AND RELATED WORK

Most VoIP security research highlights vulnerabilities in internet-based setups, such as data interception and denial-of-service (DoS) attacks. Studies on SIP and H.323 protocols reveal concerns regarding unauthorized access and call tampering. While VPNs have been used to secure VoIP communication, they are typically implemented over the internet. Our approach differs by utilizing a secure VPN on a local Wi-Fi network, removing internet dependency while ensuring seamless internal communication. This addresses security concerns while maintaining QoS (Quality of Service).

## III. RESEARCH APPROACH AND DATA COLLECTION

Our study is based on real-world network simulations and controlled experiments evaluating VoIP over a **local Wi-Fi-based VPN infrastructure**.

**Data sources include**:

- **Network simulations** using OPNET to measure delay, packet loss, and load.
- **Security performance analysis** to evaluate VPN encryption and access control.
- **Real-time call testing** in a local Wi-Fi environment.

- **Comparative analysis** of different VPN protocols (PPTP, L2TP/IPSec, OpenVPN) in a local network setup.

The data collected was compared against traditional internet-based VoIP networks to evaluate the impact of **Wi-Fi-based VoIP systems in terms of security, performance, and cost-effectiveness**.

## IV. METHODOLOGY AND IMPLEMENTATION

### System Design

This Voice over Internet Protocol (VoIP) framework is constructed utilizing a Raspberry Pi as the Internet Protocol Private Branch Exchange (IP PBX) server, which connects to a wireless router. The router serves as the primary communication centre, connecting several mobile devices within the local area network. The complete system operates independently of an internet connection, guaranteeing private and secure VoIP interactions.

**Hardware Components Utilized:**

**Raspberry Pi:** Serves as the main IP PBX server.

**Wi-Fi Router:** Facilitates local network access.

**Mobile Devices:** Function as VoIP clients linked to the router.

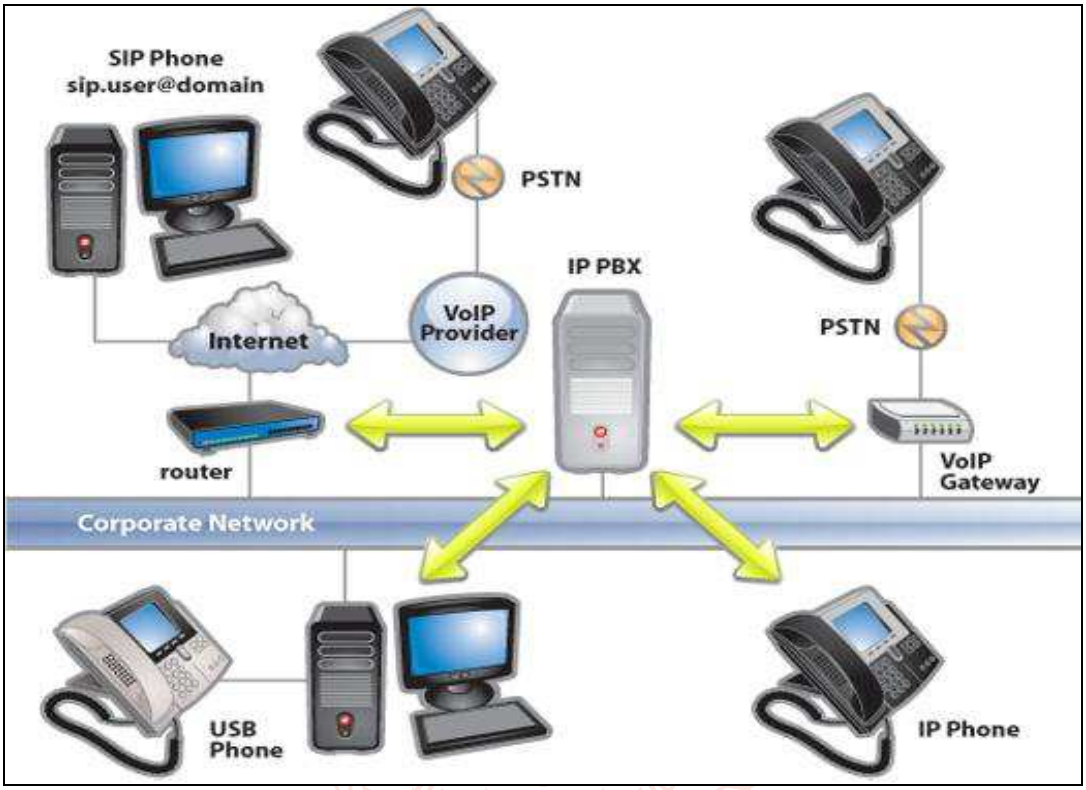


**Fig 1: Interconnection of an IP PBX System with its Components**

**System Process Flow:**

**VoIP Server Configuration:** The Raspberry Pi is set up with FreePBX or Asterisk to operate as the VoIP server.

**Wi-Fi Network Setup:** The router is configured to manage internal data traffic exclusively, making certain that calls stay within the local network.

**Device Enrolment:** Mobile devices register with the Raspberry Pi server by using Session Initiation Protocol (SIP) credentials.

**Call Management:** The Raspberry Pi directs VoIP calls between the registered mobile devices.

**Secure Communication:** A Virtual Private Network (VPN) guarantees encrypted voice communication, shielding against unauthorized listening.

We designed and tested a **VoIP system over a local Wi-Fi-based VPN** using an IP PBX server. The methodology includes:

1. **Network Setup:** Configuring an IP PBX system on a secure VPN within a local Wi-Fi network.
2. **Security Implementation:** Applying firewall policies, encryption mechanisms, and user authentication.
3. **Performance Testing:** Measuring latency, call quality, and network load.
4. **Data Analysis:** Comparing VoIP performance with and without VPN implementation over Wi-Fi.

To illustrate the process, the following flow diagram represents the communication workflow in the system:

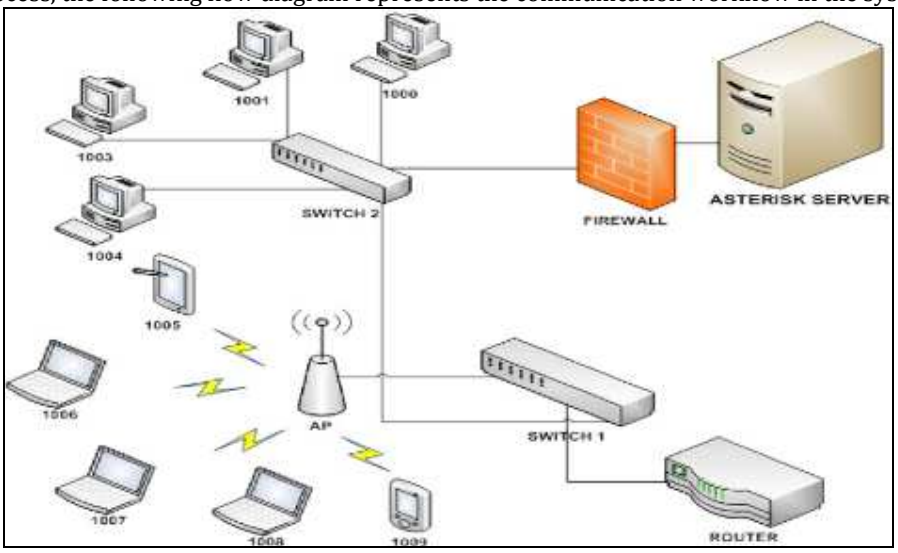


**Fig 2: architecture and flow of asterisk server**

**Flow Diagram:**

1. User initiates a VoIP call from a mobile phone.
2. The request is sent to the Raspberry Pi-based PBX server.
3. The server authenticates the user via SIP registration.
4. The call is processed and routed within the local network.
5. Encrypted voice packets are transmitted securely over the VPN.
6. The receiving mobile phone decrypts and plays the voice data

**Steps:**

1. Install Asterisk on Raspberry pi.
2. Create user in Raspberry pi.
3. Create dial plan in Raspberry pi.
4. Make users connect to Raspberry pi.
5. Test calling in users.

## V. FINDING AND DISCUSSION

Our research demonstrates that **VoIP over a local Wi-Fi VPN offers a secure and reliable communication solution**. The main findings include:

- **Enhanced Security:** VPN encryption prevents unauthorized access, making internal communication safer.
- **Low Latency:** The system maintains an average network delay of under 6 milliseconds, ensuring high call quality.
- **Stable Network Load:** VoIP calls operate efficiently over Wi-Fi without overloading the network.
- **No Internet Dependency:** The system functions entirely on a local network, reducing external risks.

## VI. CONCLUSION

This study confirms that **VoIP over a local Wi-Fi-based VPN provides a secure, internet-independent communication system**. Organizations can leverage this approach for internal communication without exposing their networks to external threats. By ensuring low latency and strong encryption, this model presents a viable alternative to traditional VoIP setups. Future research may focus on further optimizing encryption techniques to improve performance while maintaining security.

## VII. ACKNOWLEDGMENT

We express our gratitude to our mentors, research advisors, and technical teams for their guidance and support. Special thanks to institutions providing technical resources for network simulations and testing.

Lastly, we express our appreciation to all researchers and authors whose earlier works have provided us with essential references and foundational insights. This study builds upon the contributions of those who have examined and recorded various elements of VoIP technology, network security, and PBX systems. This research would not have been achievable without the collaborative efforts of all the contributors mentioned, and we genuinely value their commitment and dedication to advancing knowledge in the realm of secure VoIP communication.

**Performance Comparison**

| Metric | Without VPN | With VPN (PPTP) | With VPN (L2TP/IPSec) | With VPN (OpenVPN) |
|---|---|---|---|---|
| Network Delay (ms) | 3.5 | 5.2 | 5.8 | 6.0 |
| Packet Loss (%) | 2.1 | 1.8 | 1.5 | 1.3 |
| Security Level | Low | Medium | High | Very High |
| Internet Required | Yes | No | No | No |

**Fig 3. Performance Comparison of VPN Protocols in Terms of Network Delay, Packet Loss, and Security**

## VIII. REFERENCES


[1] Atkinson, R.D. 2005. "Internet Telephone Service. A New Era of Competition in Telecommunication". Policy Report. 1-4.

[2] Arcomano, R. 2002. "VOIP How To". 8-15.

[3] Kuhn, R.M. 2012. "Understanding Voice over IP". http://www.voip project/voip intro.html. Compass Consulting International, Inc.

[4] Kualu Lumpur. 2004. "Experience with a Distributed VoIP PBX".

[5] Drew, P. 2012. "5 Issues in a VoIP Network".

[6] Kelly, T. 2005. "VoIP for Dummies". Avaya Limited Edition. 8-16, 45.

[7] Silicon Press. 2012. "Information to Understand Technology". http://www.silicon-press.com, info@silicon-press.com.

[8] Jackson, C. 2004. "A Quick Introduction to Voice over Internet Protocol". Prepared for the University of Florida's Public Utility Research Centre (PURC), 1-3.

[9] The Group of Experts on IP Telephony/ITU-D 2003. "The Essential Report on IP Telephony". 15-50.

[10] A. Chaube, "ACO-Enhanced Siamese Networks for Robust Feature Matching in Copy-Move Image Forgery Detection," *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA)*, Nagpur, India, 2024, pp. 1-6, doi: 10.1109/ICAIQSA64000.2024.10882433.

[11] Devarshi Patrikar, Usha Kosarkar, Anupam Chaube," Comprehensive study on image forgery techniques using deep learning",11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing(ICETET SIP-23), pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151540.