Smart Telecommunication with Number Morphing Technology

P. Saibabu[1], D. Sreenivasa Rao[2] K. Yasodakumar[3], R. Jhansi[4], N.N.S.Sri Vyshnavi[5], N. Pavan Sai[6]
[1,2]*Assistant Professor, Department of ECE, Avanthi Institute of Engineering & Technology*
[3 4,5,6]*Student, Avanthi Institute of Engineering & Technology, Narsipatnam, Anakapalle.*

***Abstract*—This project proposes a Smart Telecommunication System with Number Morphing Technology to enhance privacy, security, and reliability in modern communication networks. In existing systems, caller identification is either fully visible or can be illegally spoofed, leading to privacy breaches, fraud, spam calls, and identity misuse. To address these issues, the proposed system introduces a secure and controlled number morphing mechanism that dynamically replaces the original caller number with a temporary, virtual, or encrypted number during communication. This transformation is allowed only through authenticated network authorization, ensuring that the real identity is securely stored in a centralized database and accessible only to authorized telecom authorities, thereby preventing illegal spoofing while maintaining accountability.**

The system uses encryption algorithms, secure key management, and intelligent routing protocols to protect communication data from interception and tampering. It is compatible with GSM, VoIP, SIP, and IP-based communication systems and can operate across 2G, 3G, 4G, and 5G networks. Additionally, machine learning techniques can be integrated to analyse call patterns, detect suspicious behaviour, and block fraudulent activities. The system also supports temporary number allocation for businesses, customer service platforms, online marketplaces, and delivery services. By combining privacy preservation, secure authentication, intelligent monitoring, and scalable network integration, this project offers a reliable and future-ready solution for next-generation smart communication systems.

***Index Terms*—Smart Telecommunication System, Number Morphing Technology, Caller Identity Protection, Privacy Preservation, Secure Communication, Telecommunication Security.**

I. INTRODUCTION

Telecommunication has become one of the most essential technologies in modern society. From personal communication to enterprise operations, telecommunication systems enable people and organizations to connect instantly across long distances. With the rapid development of digital technologies, communication systems are becoming smarter, more secure, and more automated. However, in many organizations such as telemarketing agencies, customer service canters, and field service companies, managing phone calls while protecting sensitive contact information remains a major challenge.

Traditional calling systems expose the actual contact numbers to callers. This can lead to misuse of customer information, privacy issues, and data leakage. Organizations need a secure system where callers can communicate with customers without accessing or storing their personal phone numbers. To address this issue, the concept of Number Morphing Technology can be implemented, where the caller interacts with contacts through a controlled system rather than directly viewing phone numbers.

The proposed project titled "Smart Telecommunication with Number Morphing Technology" aims to develop a smart calling system using a microcontroller-based communication device integrated with an Android application. The hardware device is built using an ESP32 microcontroller and a GSM communication module[1]. The Android application allows administrators to manage contact lists and assign them to authorized users. The users can initiate calls from the application without viewing the actual phone numbers.

The system uses secure authentication mechanisms such as password verification and Bluetooth connectivity to ensure only authorized users can access the device. When a user presses the call button in the mobile application, the ESP32 device receives the number through Bluetooth and initiates a call using the GSM module. The call progress, duration, and status are displayed on the device LCD and the mobile application interface.

This approach improves data privacy, prevents contact misuse, and enables efficient call management. The system also supports features such as call status monitoring, ringing detection, automatic call termination, and call duration tracking.Bycombining embedded systems, wireless communication, and mobile application technology, the proposed solution provides a cost-effective and secure telecommunication system suitable for many real-world applications such as telemarketing, survey calling, customer support, and field communication systems.

II. LITERATURE SURVEY

A literature survey is an important step in understanding the existing technologies, methodologies, and research developments related to a project. It helps identify the current solutions used in telecommunication systems, embedded systems, and secure communication technologies [6]. In the field of smalt communication systems, several technologies such as GSM communication, Internet of Things (IOT), embedded microcontrollers, and mobile applications have been used to automate calling systems and improve communication efficiency [3].

The research conducted in telecommunication systems mainly focuses on improving call automation, enhancing security, reducing infrastructure costs, and enabling remote communication control. Traditional call centre systems rely heavily on computer-based dialling software and VolP communication, which require large infrastructure and may expose sensitive customer information. Recent research has explored embedded systems and 10T technologies to build low-cost and secure communication devices [2].

The integration of microcontrollers with GSM modules has enabled the development of compact telecommunication devices capable of making voice calls, sending messages, and monitoring call status. Similarly, mobile applications and wireless technologies such as Bluetooth allow remote control of these devices, creating flexible and user-friendly communication systems[4].

The literature survey also highlights the need for improved privacy protection in telecommunication systems. Many organizations face issues related to contact data leakage, unauthorized access to phone numbers, and misuse of customer information [12].

As a result, researchers are exploring solutions that hide or mask contact numbers from users while still allowing communication.

The proposed project builds upon these research areas by combining embedded hardware, GSM communication, Bluetooth connectivity, and mobile application technology to develop a secure telecommunication system with number morphing functionality.

III. PROPOSED SYSTEM

To overcome the limitations of traditional telecommunication systems, the proposed project introduces a Smart Telecommunication System with Number Morphing Technology. The system ensures that callers can communicate with customers without accessing their phone numbers. This improves data privacy and enhances security [5].

The proposed system consists of a hardware communication device and a mobile application. The hardware device is built using an ESP32 microcontroller integrated with aGSM module. The ESP32 receives call requests from the Android application through Bluetooth communication and automatically places the call using the GSM network. A keypad- based password authentication system is implemented in the device to prevent unauthorized access. Only authorized users who enter the correct password can connect the device to the mobile application via Bluetooth. Once connected, the device waits for call instructions from the application. The Android application contains two modules: the administrator module and the user module. The administrator can manage contact information and assign specific contacts to different users. This ensures that callers only access the contacts assigned to them [7].

When a user selects a contact in the application and presses the call button, the phone number is transmitted securely to the ESP32 device. The GSM module then dials the number while the LCD screen displays call status messages such as "Calling", "Ringing", "Call Connected", and "Call Ended". The application displays only the contact's name and call duration to the user, hiding the actual phone number. This system ensures that the caller never sees or stores the customer's phone number, thereby preventing misuse of sensitive information.

Advantages of Proposed System

- Protects customer phone numbers from being exposed to callers.
- Provides secure password-based device authentication.
- Enables centralized contact management through the admin panel.
- Reduces risk of contact data misuse
- Provides real-time call status monitoring.
- Uses cost-effective embedded hardware components.

3.1 BLOCK DIAGRAM

The figure1. Shows the block diagram illustrates the overall architecture of the smart telecommunication system and shows how different components interact with each other.

The Power Supply block provides the required electrical power to the entire system. It ensures stable voltage for the microcontroller, GSM module, and other electronic components [8].

The Controller MCU is the central processing unit of the system. It is responsible for controlling all system operations. The microcontroller processes commands received from the mobile application and communicates with the GSM module to initiate phone calls. It also monitors call status and updates the display.

The GSM Module is connected to the controller through serial communication. It enables the system to make voice calls using the cellular network. When the microcontroller sends a dialling command, the GSM module connects to the mobile network and establishes the call.[9]

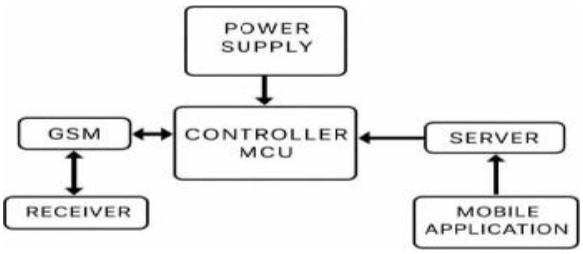

Figure1: Block diagram of smart telecommunication system

The Server acts as a centralized data management system. It stores user accounts, contact lists, and call assignments. The server ensures that administrators can assign specific contacts to users securely [14].

The Mobile Application interacts with the server to retrieve contact information and display it to the user. When a user selects a

contact and presses the call button, the application sends the call request to the controller. The controller then processes the request and instincts the GSM module to dial the number [10].

Overall, the block diagram shows the communication flow between the power supply, controller, GSM module, server, and mobile application to perform secure call operations [11].

IV. OUTPUTS

Figure2: Outputs

Figure2 shows the device setup, mobile app, call initiation and call status display[13].

- Device Setup – The smart telecommunication device is powered on and ready to work, showing initial details on the display.

- Mobile App Connection – The device connects with the mobile application, allowing the user to control and manage calls.
- Call Initiation – The user starts a call, and the system activates number morphing to hide the original number.
- Call Status Display – The device shows the call status (like "Calling…"), indicating that the secure communication is in progress.

V. CONCLUSION

The Smart Telecommunication with Number Morphing Technology project successfully demonstrates a secure and efficient communication system using embedded hardware and mobile application integration. The system combines a microcontroller-based hardware device with GSM communication technology to create a smart calling platform that protects sensitive contact information.

The developed system allows administrators to assign contact lists to users through a mobile application while ensuring that the caller cannot view the actual phone numbers. Instead, the user interface only displays the contact's name and call duration, thereby preventing misuse of customer information. The integration of password authentication, Bluetooth communication, and GSM-based calling ensures secure and controlled communication.

The proposed system provides a cost-effective solution compared to traditional telecommunication systems. By using embedded hardware such as the ESP32 microcontroller and GSM module, the system reduces infrastructure requirements while maintaining reliable communication. The project demonstrates the potential of IOT and embedded technologies in developing smart and secure telecommunication solutions for modern organizations.

REFERENCES

[1] Neeraj Bhargava and Ritu Bhargava, "Secure Communication in GSM Networks," *International Journal of Computer Applications*, vol. 96, no. 15, pp. 25–30, 2014.

[2] Hossen A. Mustafa, M. Z. Shafiq, and A. X. Liu, "Detection and Prevention of Caller ID Spoofing Attacks in VoIP Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2562–2574, 2017

[3] Wei Zhang and Xiaofei Wang, "Secure GSM-SIP Interworking Architecture for Smart Telecommunication Systems," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 66–72, 2016.

[4] Ming Li et al., "Privacy Preservation in Mobile Communication Networks," *IEEE Access*, vol. 8, pp. 112345–112356, 2020.

[5] Ayman E. Khedr et al., "An Efficient Secure Communication Framework for Smart Systems," *International Journal of Communication Systems*, vol. 34, no. 9, 2021

[6] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*, Elsevier, 2016.

[7] Hossen A. Mustafa, M. Z. Shafiq, and A. X. Liu, "Detection and Prevention of Caller ID Spoofing Attacks in VoIP Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2562–2574, 2017.

[8] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*, Elsevier, 2016.

[9] Rajesh Kumar and S. Patel, "IoT-Based Smart Communication System Using GSM and Embedded Controllers," *International Journal of Computer Applications*, vol. 178, no. 7, pp. 23–28, 2019.

[10] Neeraj Bhargava and Ritu Bhargava, "Secure GSM Communication Techniques for Modern Telecommunication Networks," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 3, no. 5, pp. 1450–1455, 2014.

[11] Ayman E. Khedr et al., "A Secure Embedded Communication System for Smart Telephony Applications," *International Journal of Communication Systems*, vol. 34, no. 9, pp. 1–15, 2021.

[12] Shen Wang: Caller ID Verification Across Heterogeneous Networks Using Challenge Response Mechanism https://doi.org/10.1145/3625 546.

[13] K. Ashton, "That 'Internet of Things' Thing," RFID Journal, 2009.

[14] M. Collotta and G. Pau, “A Novel IoT-based Smart Communication System,” IEEE Sensors Journal, 2015.