# Secure Bluetooth Device Authentication Using OTP

Ankita Gonjari [1], Saniya Gaikwad[2], Manasi Amrule[3], Anuja Hake[4], Akanksha Kole[5]
[1,2,3,4,5]*Department of Computer Science and Engineering, Yashoda Technical Campus, Faculty of Engineering, Satara, Maharashtra, India*

***Abstract*—Bluetooth technology is widely used in smartphones, wearable devices, smart home systems, healthcare devices, and industrial Internet of Things applications. Even though Bluetooth communication provides easy wireless connectivity, traditional pairing methods such as static PINs and automatic pairing are vulnerable to security threats like unauthorized access, replay attacks, eavesdropping, and device impersonation. These security issues can affect the confidentiality and reliability of data communication between devices.**

**The proposed system introduces a secure Bluetooth authentication mechanism using One-Time Password (OTP) verification. In this system, a unique OTP is generated during every authentication session and remains valid only for a short period of time. The Bluetooth connection is established only after successful OTP verification, which adds an additional security layer to the standard pairing process.**

**The system improves security by preventing attackers from reusing previously captured credentials. OTP-based authentication also reduces the chances of unauthorized device access and improves secure communication between Bluetooth-enabled devices. The proposed solution is lightweight, efficient, and suitable for modern IoT environments where secure wireless communication is important.**

***Index Terms*—Bluetooth Security, One-Time Password, OTP Authentication, Secure Pairing, Internet of Things, Wireless Communication, Bluetooth Authentication**

## I. INTRODUCTION

Bluetooth communication has become an important part of modern wireless technology. It is commonly used in smartphones, laptops, wearable devices, smart home systems, healthcare devices, and industrial automation applications. Bluetooth provides low-cost and low-power wireless communication, making it suitable for short-range data transfer between devices. Although Bluetooth technology is widely used, security remains a major concern during device pairing and communication. Traditional Bluetooth authentication methods such as fixed PIN-based pairing or "Just Works" pairing provide limited protection against modern cyber threats. Attackers can exploit these weak authentication mechanisms to gain unauthorized access to devices, intercept confidential information, or perform replay and man-in-the-middle attacks.

As Bluetooth-enabled devices continue to increase in IoT ecosystems, the need for stronger authentication methods has become essential. A secure and dynamic authentication mechanism can significantly improve communication security and protect sensitive data from unauthorized users.

The proposed system introduces OTP-based authentication for Bluetooth device pairing. In this approach, a temporary One-Time Password is generated for every connection request. The OTP remains valid only for a limited time and must be entered correctly before the Bluetooth connection is established. This dynamic authentication process improves security compared to static passwords and reduces the risk of unauthorized access.

The system is designed to provide better protection while maintaining simplicity and low computational overhead. It can be effectively implemented in smart devices, healthcare systems, secure file transfer applications, and industrial IoT environments.

## II. PROBLEM STATEMENT

Bluetooth technology is widely used for wireless communication, but traditional authentication methods are not fully secure. Static PINs and automatic pairing mechanisms can be easily targeted by attackers. These weak security methods allow risks such as unauthorized access, replay attacks,

eavesdropping, and device impersonation.

Many Bluetooth-enabled devices operate in public or untrusted environments where attackers may intercept communication or gain unauthorized control over connected devices. Existing Bluetooth pairing methods do not provide sufficient dynamic security for modern applications.

There is a need for a stronger authentication mechanism that can improve Bluetooth security without increasing system complexity. The proposed system addresses this problem by integrating OTP-based authentication into the Bluetooth pairing process to ensure secure and reliable communication

## III. OBJECTIVES

The main objectives of the proposed system are:

1. To design and implement a secure Bluetooth authentication system using OTP verification.
2. To prevent unauthorized Bluetooth device pairing and access.
3. To improve data confidentiality and secure wireless communication.
4. To reduce the risks of replay attacks, eavesdropping, and device impersonation.
5. To generate dynamic session-based authentication for every Bluetooth connection.
6. To provide a lightweight and efficient security mechanism suitable for IoT devices.
7. To maintain ease of use while improving Bluetooth communication security.

## IV. LITERATURE SURVEY

Bluetooth security has become an important topic because many wireless devices use Bluetooth communication in daily applications. Researchers have identified several weaknesses in traditional Bluetooth pairing methods such as static PINs and weak authentication systems.

Levi and Wool explained relay attacks in Bluetooth communication and showed how attackers can access devices by exploiting weak authentication. Liu and Zhu proposed Bluetooth-based mobile authentication methods to improve communication security.

Recent research on OTP authentication systems shows that dynamic passwords provide better security than fixed passwords and reduce replay attacks. Studies on Bluetooth Low Energy security also highlight risks such as unauthorized access and eavesdropping.

The reviewed literature indicates that OTP-based authentication can improve Bluetooth security and provide safer communication between wireless devices.

## V. PROPOSED METHODOLOGY

The proposed system enhances Bluetooth communication security by integrating One-Time Password authentication into the device pairing process.

### A. System Overview

The system consists of two Bluetooth-enabled devices where one device generates a temporary OTP for authentication. The OTP is shared securely with the authorized user and verified before establishing the Bluetooth connection.

The complete authentication process includes:

- Bluetooth connection request
- OTP generation
- OTP transmission
- OTP verification
- Secure connection establishment

Only after successful OTP verification will the system allow communication between devices.

### B. OTP Generation

The system generates a random One-Time Password whenever a new Bluetooth pairing request is initiated. The OTP remains valid only for a short duration to improve security.

Features of OTP generation include:

- Session-based authentication
- Time-limited validity
- Randomized secure code generation

This prevents attackers from reusing old authentication credentials

### C. Bluetooth Authentication Process

The authentication process works in the following steps:

1. The user initiates Bluetooth pairing.
2. The system generates a temporary OTP.
3. The OTP is displayed or transmitted securely.
4. The user enters the OTP into the target device.
5. The system verifies the entered OTP.
6. If verification is successful, the Bluetooth connection is established.

7. If the OTP is incorrect, access is denied.

This process adds an additional layer of security to the standard Bluetooth pairing mechanism.

D. Security Features

The proposed system includes multiple security features:

- Dynamic OTP verification
- Limited retry attempts
- Session-based authentication
- Prevention of replay attacks
- Reduced risk of unauthorized access
- Secure communication between devices

These features improve Bluetooth security without significantly increasing system complexity.

E. Hardware and Software Requirements Hardware Requirements

- Arduino Uno / ESP32
- HC-05 or HC-06 Bluetooth Module
- Smartphone or Laptop
- Power Supply
- Optional LCD or OLED Display

Software Requirements

- Arduino IDE
- Python / Java / C++
- Bluetooth Communication Libraries
- OTP Generation Algorithm
- Windows or Linux Operating System

## VI. EXPECTED RESULTS


The proposed system is expected to provide the following results:

- Improved Bluetooth communication security
- Prevention of unauthorized device access
- Secure and reliable OTP-based authentication
- Reduced replay attacks and eavesdropping risks
- Better protection compared to static PIN-based pairing
- Lightweight and efficient performance for IoT devices
- Easy integration with existing Bluetooth systems

The OTP-based Bluetooth authentication system will create a safer communication environment for wireless devices. Since every OTP is temporary and session-based, attackers cannot reuse old credentials or easily predict future passwords.

The proposed system can be effectively used in smart home systems, healthcare devices, secure file transfer applications, wearable devices, industrial IoT systems, and access control applications.

## VII. CONCLUSION

The proposed Bluetooth device authentication system using One-Time Password provides a secure and efficient solution for improving wireless communication security. Traditional Bluetooth pairing methods rely on static PINs and weak authentication mechanisms, which are vulnerable to unauthorized access and various cyberattacks.

The integration of OTP-based authentication adds an additional layer of security by generating dynamic and temporary passwords for every connection session. This reduces the risks of replay attacks, eavesdropping, and unauthorized device pairing.

The proposed system is lightweight, easy to implement, and suitable for modern IoT environments where secure wireless communication is essential. It maintains user convenience while improving authentication reliability and data confidentiality.

In the future, the system can be further enhanced by integrating biometric authentication, mobile application support, cloud-based monitoring, and advanced encryption techniques to provide even stronger Bluetooth security.

## REFERENCES

[1] Y. Levi and A. Wool, “Relay Attacks on Bluetooth Authentication and Solutions,” Proc. Security and Privacy in Communication Networks, 2004.

[2] J. Liu and Y. Zhu, “Research on Mobile Phone Based Authentication via Bluetooth,” Proc. International Conference on Mechatronics,

Electronic, Industrial and Control Engineering, 2015.

[3] B. Bartłomiejczyk and M. El Fray, "Device Risk Analysis Protocol for SMS-Based OTP Authentication," IEEE Access, 2024.

[4] S. Kumar and R. Singh, "OTP-Based Authentication System: A Review," International Journal of Computer Applications, vol. 185, no. 12, pp. 10–15, 2024.

[5] A. Sharma and P. Gupta, "Securing Bluetooth Low Energy: A Literature Review," International Journal of Network Security, vol. 26, no. 2, pp. 100–110, 2024.

[6] R. Kumar and S. Patil, "Secure Wireless Communication using Dynamic Authentication Systems," Journal of Advanced Computing Research, vol. 18, no. 3, pp. 201–210, 2023.

[7] M. Shah and P. Deshmukh, "IoT Device Authentication using OTP and Encryption Techniques," International Journal of Smart Technology and Engineering, vol. 9, no. 4, pp. 56–64, 2024.

[8] N. Verma and K. Joshi, "Security Challenges in Bluetooth-Based IoT Systems," IEEE International Conference on Wireless Communication and Security, 2023.

[9] D. Mehta and A. Kulkarni, "Lightweight Authentication Mechanisms for Smart Devices," International Journal of Computer Science and Information Security, vol. 20, no. 5, pp. 75–82,2023.

[10] P. Singh and V. Rao, "Secure Pairing Mechanisms for Bluetooth Low Energy Devices," Journal of Network and Information Security, vol. 14, no. 1, pp. 33–41, 2024