**QR**

Good morning, everyone. I am [PANGALAN NATIN], and today we will be presenting our research titled '**Secure Boot Authentication: Implementing a QR-Based Access Control System for Computer Startup**.'

**Introduction**

In today’s digital age, securing computer systems from unauthorized access is critical. Traditional security methods, such as Secure Boot, protect the system only after it has started. However, there is a significant gap in security before the operating system boots up. Our research addresses this issue by introducing a QR code-based pre-boot authentication system that ensures the computer will not power on until a valid QR code is authenticated. This method provides an additional layer of security by preventing any unauthorized access right from the startup.

**Statement of the Problem**

The main problem our research tackles is the lack of pre-boot authentication mechanisms. Traditional methods allow the computer to power on without verifying the user’s identity, which poses a security risk. Our proposed solution introduces a QR-based authentication system that requires user verification before the system boots, thereby preventing unauthorized users from accessing or tampering with the computer even before the operating system loads.

**Objectives of the Study**

Our general objective is to enhance computer security by implementing a QR code-based pre-boot authentication system. This system ensures that only users with valid QR codes can initiate the computer's startup process.

The specific objectives are:

1. To design and implement a QR code-based authentication system integrated with the computer’s hardware and startup process.
2. To evaluate the effectiveness of this system in preventing unauthorized access.
3. To assess the impact of this authentication system on user experience and identify potential improvements.

**Scope and Limitation**

The scope of this study covers the design, implementation, and evaluation of the QR code-based pre-boot authentication system. We will focus on integrating the system with the computer’s hardware and firmware to ensure secure access control.

Limitations include:

* Hardware Compatibility: The system’s effectiveness depends on compatibility with various hardware configurations, which may limit its applicability across different devices.
* Security Testing Scope: The study will be conducted in a controlled environment, which may not fully reflect real-world scenarios.
* User Experience Variability: The user experience evaluation is based on a limited sample and may not cover all possible user interactions.

**Significance of the Study**

This study is significant because it introduces a new approach to pre-boot authentication, filling a crucial gap in current security protocols. By requiring QR code verification before the computer powers on, we can greatly reduce the risk of unauthorized access and potential security breaches. This system is particularly beneficial for environments with high-security requirements, contributing to overall system integrity and data protection.

**Methodology**

Our methodology involves designing and implementing a QR code-based authentication system that integrates with the computer’s startup process. We tested the system’s effectiveness in preventing unauthorized access and evaluated its impact on user experience. The results show a significant improvement in pre-boot security compared to traditional methods.

**Conclusion and Recommendations**

In conclusion, our research demonstrates that a QR code-based pre-boot authentication system effectively enhances computer security by preventing unauthorized access right from the startup. We recommend further research to address hardware compatibility and explore additional security features, such as integrating biometric authentication for even greater security.